明　細　書

著作物保護システム、記録装置、再生装置及び記録媒体

DIGITAL WORK PROTECTION SYSTEM, RECORDING APPARATUS, REPRODUCTION APPARATUS, AND RECORDING MEDIUM

技術分野

本発明は、デジタルデータを大容量の記録媒体に記録し再生する技術に関し、特に不正装置によるコンテンツの不正な記録及び不正な再生を防止する技術に関する。

背景技術

近年、マルチメディア関連技術の発展、大容量記録媒体の出現等を背景として、動画、音声等からなるデジタルコンテンツ（以下、コンテンツ）を生成して、光ディスク等の大容量記録媒体に格納して配布し、又はネットワークを介して配布するシステムが普及しつつある。

配布されたコンテンツは、コンピュータや再生装置等で読み出され、再生、又は複製の対象となる。

一般的に、コンテンツの著作権を保護するため、即ちコンテンツの不正再生や不正コピーなどの不正利用を防止するために暗号化技術が用いられる。具体的には、記録装置は、コンテンツを暗号化鍵を用いて暗号化して光ディスク等の記録媒体に記録して配布する。これに対して、その暗号化鍵に対応する復号鍵を保有する再生装置のみが、記録媒体から読み出した暗号化コンテンツをその復号鍵を用いて復号して、コンテンツの再生等を行うことができる。

なお、コンテンツを暗号化して記録媒体に記録する際には、再生装置が保有する復号鍵に対応する暗号化鍵を用いて、コンテンツそのものを暗号化して記録する方法や、コンテンツをある鍵で暗号化して記録した上で、その鍵に対応する復号用の鍵を、再生装置が保有する復号鍵に対応する暗号化鍵で暗号化して記録する方法等が用いられる。

このとき、再生装置が保有する復号鍵は外部に露見しないように厳重に管理される必要があるが、不正者による当該再生装置内部の不正な解析により、復号鍵が外部に暴露される危険性がある。復号鍵が一旦不正者により暴露されてしまうと、前記不正者は、コンテンツを不正利用する記録装置、再生装置を製造して不法に販売したり、又はコンテンツを不正利用するためのコンピュータプログラムを作成し、インターネット等によりこのようなプログラムを流布することが考えられる。

このような場合、著作権者は一旦暴露された復号鍵では、次から提供するコンテンツを扱えないようにしたいと考える。このようなことを実現する技術を鍵無効化技術と呼び、特許文献１により鍵無効化を実現するシステムが開示されている。

従来の鍵無効化技術では、予め、記録媒体の書き換え不可領域に、装置の保有する鍵が無効化されていることを示す鍵無効化情報を記録している。装置は、記録媒体に記録されている鍵無効化情報を用いて、当該装置の保有する鍵が無効化されているか否かを判断し、無効化された鍵を保有する場合には、当該装置は、前記記録媒体を利用することができないようにしている。また、新たに鍵の無効化が発生すると、前記の鍵無効化情報は更新され、この無効化発生以降に製造される新たな記録媒体には更新後の鍵無効化情報が記録される。こうして無効化された鍵では新たな記録媒体を利用できない仕組みとなっている。

一方、光ディスク等の記録媒体に記録されているコンテンツの読み出し、あるいは書き込みは、光ディスクドライブと称されるパソコン周辺機器で行われることが一般的であるが、機器の互換性を達成するためにその入出力の方法は公開の情報として標準化され、秘密にされないことが一般的である。このため、記録媒体に記録されているコンテンツは、パソコン等により、容易に読み出すことが可能であり、また、読み出したデータを他の記録媒体に書き込むことも容易である。したがって、コンテンツの著作権を保護するシステムにおいては、記録媒体上のデータを読み出し、他の記録媒体に書き込むという、通常のユーザが行い得る行為に対して、それを防止する有効な機能を備えるシステムでなければならない。記録媒体から読み出したデータが他の記録媒体に書き込まれることを防止する技術をメディアバインド技術と呼び、特許文献２により、メ

ディアバインドを実現するメカニズムが開示されている。

従来のメディアバインド技術を利用して著作権保護を実現するために、予め、記録媒体の書き換え不可領域には、記録媒体を識別する媒体識別子が記録されており、当該記録媒体に記録されている暗号化コンテンツは、この媒体識別子に基づいて、暗号化されている。従って、暗号化コンテンツだけを他の記録媒体に複製しても、他の記録媒体は、別の媒体識別子を記録しており、この別の媒体識別子に基づいて、暗号化コンテンツを正しく復号することはできない。

（発明が解決しようとする課題）

しかしながら、コンテンツの不正な利用の拡大を防ぐために、多様な不正防止技術の実現が要望されている。

（特許文献１）

特開２００２－２８１０１３号公報

（特許文献２）

特許第３０７３５９０号公報

（特許文献３）

特開平０９－１６０４９２号公報

発明の開示

本発明は、上記の要望に対処するために、コンテンツの不正利用を防止することができる著作物保護システム、記録装置、記録方法、再生装置、再生方法、コンピュータプログラム及び記録媒体を提供することを目的とする。

上記目的を達成するために本発明は、記録媒体にコンテンツを暗号化して書き込む記録装置と、前記記録媒体に記録されている暗号化コンテンツの復号を試みる複数の再生装置とから構成される著作物保護システムである。

前記複数の再生装置のうちいずれか１台以上は、無効化されている。

前記記録媒体は、読出専用の書換不可領域と、読出し及び書込みの可能な書換可能領域とを備え、前記書換不可領域には、当該記録媒体に固有の媒体固有番号が予め記録されている。

前記記録装置は、無効化されていない各再生装置についてメディア鍵が、無効化された各再生装置について所定の検知情報が、それぞれ、当該再生装置の

デバイス鍵を用いて、暗号化されて生成された複数の暗号化メディア鍵から構成されるメディア鍵データを記憶している記憶手段と、前記記録媒体の前記書換不可領域から前記媒体固有番号を読み出す読出手段と、読み出した前記媒体固有番号及び前記メディア鍵に基づいて、暗号化鍵を生成する生成手段と、生成された前記暗号化鍵に基づいて、デジタルデータであるコンテンツを暗号化して暗号化コンテンツを生成する暗号化手段と、前記記憶手段から前記メディア鍵データを読み出す読出手段と、読み出された前記メディア鍵データ及び生成された前記暗号化コンテンツを前記記録媒体の前記書換可能領域に書き込む書込手段とを備えている。

各再生装置は、前記記録媒体の前記書換可能領域に書き込まれたメディア鍵データから当該再生装置に対応する暗号化メディア鍵を読み出す読出手段と、当該再生装置のデバイス鍵を用いて、読み出された前記暗号化メディア鍵を復号して復号メディア鍵を生成する復号手段と、生成された復号メディア鍵が、前記検知情報であるか否かを判断し、前記検知情報である場合に、前記記録媒体に記録されている暗号化コンテンツの復号を禁止し、前記検知情報でない場合に、暗号化コンテンツの復号を許可する制御手段と、復号が許可された場合に、前記記録媒体から前記暗号化コンテンツを読み出し、生成された復号メディア鍵に基づいて、読み出した前記暗号化コンテンツを復号して復号コンテンツを生成する復号手段とを備える。

（発明の効果）

この構成よると、前記記録装置は、無効化されていない各再生装置についてメディア鍵が、無効化された各再生装置について所定の検知情報が、それぞれ、当該再生装置のデバイス鍵を用いて、暗号化されて生成された複数の暗号化メディア鍵から構成されるメディア鍵データを記録媒体に書き込み、また、媒体固有番号及びメディア鍵に基づいて、生成された暗号化鍵を生成し、生成された前記暗号化鍵に基づいて、生成された暗号化コンテンツを記録媒体に書き込む。また、再生装置は、デバイス鍵を用いて、暗号化メディア鍵を復号して復号メディア鍵を生成し、生成した復号メディア鍵が、前記検知情報である場合に、前記記録媒体に記録されている暗号化コンテンツの復号を禁止する。

このように構成されているので、無効化された再生装置を排除することがで

きる。

ここで、別の記録媒体は、無効化されていない各再生装置についてメディア鍵が、無効化された各再生装置について所定の検知情報が、それぞれ、当該再生装置のデバイス鍵を用いて、暗号化されて生成された複数の別の暗号化メディア鍵から構成される別のメディア鍵データを記憶している。前記記録装置は、さらに、前記別の記録媒体に記憶されている別のメディア鍵データと、前記記憶手段に記憶されている前記メディア鍵データとの新旧を比較する比較手段と、前記別のメディア鍵データの方が新しいと判断される場合に、前記別の記録媒体から前記別のメディア鍵データを読み出し、読み出した前記別のメディア鍵データを、前記記憶手段に記憶されている前記メディア鍵データに、上書きする更新手段とを備え、前記読出手段は、前記メディア鍵データの読出しに代えて、前記記憶手段から前記別のメディア鍵データを読み出し、前記書込手段は、前記メディア鍵データの書込みに代えて、読み出された前記別のメディア鍵データを前記記録媒体の前記書換可能領域に書き込む。

この構成によると、記録装置は、内部に記憶しているメディア鍵データを、別の記録媒体から取得した別の暗号化メディア鍵に更新することができる。

ここで、前記記憶手段は、さらに、当該記録装置及び前記複数の再生装置のいずれかに割り当てられた公開鍵が無効化されていることを示す無効化データを記憶しており、前記記録装置は、さらに、前記無効化データに対してデジタル署名を施して検証情報を生成する署名生成手段を備え、前記書込手段は、さらに、生成した前記検証情報を前記記録媒体の前記書換可能領域に書き込む。また、前記記録装置は、さらに、当該記録装置及び前記複数の再生装置のいずれかに割り当てられた公開鍵が無効化されていることを示す無効化データを記憶しており、前記無効化データに対してデジタル署名を施して検証情報を生成し、生成した前記検証情報を前記記録媒体の前記書換可能領域に書き込み、前記読出手段は、さらに、前記記録媒体の前記書換可能領域に書き込まれた前記検証情報を読み出し、前記再生装置は、さらに、読み出した前記検証情報に基づいて、署名検証を施して、検証の成功又は失敗を示す検証結果を出力する検証手段を備え、前記制御手段は、さらに、前記検証結果が検証の失敗を示す場合に、前記暗号化コンテンツの復号を禁止し、前記検証結果が検証の成功を示

す場合に、前記暗号化コンテンツの復号を許可する。

この構成によると、記録装置は、さらに、デジタル署名により生成した検証情報を記録媒体に書き込むので、再生装置において、検証情報を検証することにより、不正な再生装置を排除することができる。

ここで、前記記憶手段は、さらに、当該記録装置の公開鍵証明書を記憶しており、前記読出手段は、さらに、前記記憶手段から前記公開鍵証明書を読み出し、前記書込手段は、読み出された前記公開鍵証明書を前記記録媒体の前記書換可能領域に書き込む。また、前記記録装置は、さらに、当該記録装置の公開鍵証明書を記憶しており、前記公開鍵証明書を読み出し、読み出した前記公開鍵証明書を前記記録媒体の前記書換可能領域に書き込み、前記再生装置は、さらに、前記記録装置及び前記複数の再生装置のいずれかに割り当てられた公開鍵が無効化されていることを示す第１無効化データを記憶している記憶手段と、前記記録媒体から前記公開鍵証明書を読み出す証明書読出手段と、読み出した公開鍵証明書に含まれる公開鍵が、前記第１無効化データにより、無効化されていることを示しているか否かを検証する公開鍵検証手段とを含み、前記制御手段は、さらに、前記公開鍵が無効化されている場合に、前記暗号化コンテンツの復号を禁止し、前記公開鍵が無効化されていない場合に、前記暗号化コンテンツの復号を許可する。

この構成によると、記録装置は、公開鍵証明書を記録媒体に書き込み、再生装置は、記録媒体から公開鍵証明書を読み出し、公開鍵が無効化されている場合に、暗号化コンテンツの復号を禁止できる。

ここで、別の記録媒体は、前記記録装置及び前記複数の再生装置のいずれかに割り当てられた公開鍵が無効化されていることを示す第２無効化データを記憶しており、前記再生装置は、さらに、前記別の記録媒体に記憶されている前記第２無効化データと、前記記憶手段に記憶されている前記第１無効化データとの新旧を比較する比較手段と、前記第２無効化データの方が新しいと判断される場合に、前記別の記録媒体から前記第２無効化データを読み出し、読み出した前記第２無効化データを、前記記憶手段に記憶されている前記第１無効化データに、上書きする更新手段とを含む。

この構成によると、再生装置は、無効化データを最新の状態に更新すること

ができる。

ここで、前記記憶手段は、さらに、当該記録装置を識別する装置識別子を記憶しており、前記記録装置は、さらに、前記記憶手段から前記装置識別子を読み出し、読み出した前記装置識別子を前記コンテンツに電子透かしとして埋め込む埋込手段を備え、前記暗号化手段は、前記装置識別子が埋め込まれたコンテンツを暗号化する。また、前記再生装置は、さらに、当該再生装置を識別する装置識別子を記憶している前記記憶手段と、復号が許可された場合に、前記記憶手段から前記装置識別子を読み出し、読み出した前記装置識別子を前記暗号化コンテンツに電子透かしとして埋め込む埋込手段と、前記装置識別子が埋め込まれた前記暗号化コンテンツを前記記録媒体に書き込む。

記録装置及び再生装置は、装置識別子が埋め込こまれたコンテンツを記録媒体に書き込むので、前記コンテンツが不正に流通した場合に、前記コンテンツから、埋め込まれた装置識別子を抽出することにより、そのコンテンツを記録した記録装置及び再生装置を特定することができる。

ここで、前記記憶手段に記憶されている前記メディア鍵データは、さらに、当該メディア鍵データを識別するデータ識別子を含み、前記書込手段は、前記データ識別子と前記暗号化コンテンツとを対応付けて、前記記録媒体の前記書換可能領域に書き込み、前記データ識別子を含む前記メディア鍵データを前記書換可能領域に書き込む。また、前記記録装置に記憶されている前記メディア鍵データは、さらに、当該メディア鍵データを識別するデータ識別子を含み、前記記録装置は、前記データ識別子と前記暗号化コンテンツとを対応付けて、前記記録媒体の前記書換可能領域に書き込み、前記データ識別子を含む前記メディア鍵データを前記書換可能領域に書き込み、前記再生装置は、さらに、前記記録媒体に記録されている前記暗号化コンテンツの指定を受け付ける受付手段と、指定が受け付けられた前記暗号化コンテンツに対応付けられた前記データ識別子を前記記録媒体から読み出す読出手段と、読み出した前記データ識別子を含む前記メディア鍵データを前記記録媒体から読み出す読出手段とを含み、前記制御手段は、読み出した前記メディア鍵データに基づいて、前記暗号化コンテンツの復号の可否を判断する。

記録装置は、前記データ識別子と前記暗号化コンテンツとを対応付けて、前

記記録媒体に書き込み、前記データ識別子を含む前記メディア鍵データを前記記録媒体に書き込むので、再生装置において、データ識別子を介して、暗号化コンテンツに対応するメディア鍵データを取得し、取得したメディア鍵データに基づいて、暗号化コンテンツの復号の許否を判断できる。

図面の簡単な説明

図１は、コンテンツ供給システム１０の構成を示す構成図である。

図２は、記録装置１００の構成を示すブロック図である。

図３は、記録媒体１２０に記録されているデータの構造を示すデータ構造図である。

図４は、再生装置２００の構成を示すブロック図である。

図５は、記録装置１００による記録媒体１２０へのデータの書き込みの動作を示すフローチャートである。

図６は、再生装置２００による記録媒体１２０に記録されているデータの再生の動作を示すフローチャートである。図７へ続く。

図７は、再生装置２００による記録媒体１２０に記録されているデータの再生の動作を示すフローチャートである。図６から続く。

図８は、第１の実施の形態の変形例におけるｎ枚の記録媒体に記録されているデータの構造を示すデータ構造図である。

図９は、第１の実施の形態の変形例における記録媒体に記録されているデータの構造を示すデータ構造図である。

図１０は、コンテンツ供給システム２０の構成を示す構成図である。

図１１は、記録装置１１００の構成を示すブロック図である。

図１２は、記録媒体１３００に記録されているデータの構造を示すデータ構造図である。

図１３は、再生装置１２００の構成を示すブロック図である。

図１４は、記録媒体１３００ａに記録されているデータの構造を示すデータ構造図である。

図１５は、記録媒体１３００ｂに記録されているデータの構造を示すデータ構造図である。

図１６は、記録装置１１００による記録媒体１３００へのデータの書き込みの動作を示すフローチャートである。図１７へ続く。

図１７は、記録装置１１００による記録媒体１３００へのデータの書き込みの動作を示すフローチャートである。図１８へ続く。

図１８は、記録装置１１００による記録媒体１３００へのデータの書き込みの動作を示すフローチャートである。図１７から続く。

図１９は、再生装置１２００による記録媒体１３００に記録されているデータの再生の動作を示すフローチャートである。図２０へ続く。

図２０は、再生装置１２００による記録媒体１３００に記録されているデータの再生の動作を示すフローチャートである。図１９から続く。

発明を実施するための最良の形態

１．第１の実施の形態

本発明に係る１の実施の形態としてのコンテンツ供給システム１０について説明する。

１．１　コンテンツ供給システム１０の構成

コンテンツ供給システム１０は、図１に示すように、コンテンツサーバ装置５００、記録装置１００及び再生装置２００ａ、２００ｂ、２００ｃ、２００ｄ、２００ｅ、・・・から構成されている。記録装置１００及び再生装置２００ａ、２００ｂ、２００ｃ、２００ｄ、２００ｅ、・・・の台数の合計は、ｎ台である。記録装置１００には、装置番号「１」が割り当てられており、再生装置２００ａ、２００ｂ、２００ｃ、２００ｄ、２００ｅ、・・・には、それぞれ、装置番号「２」、「３」、「４」、・・・、「ｎ」が割り当てられている。各装置は、割り当てられた各装置番号により識別される。

これらのｎ台の装置のうち、再生装置２００ｂ及び再生装置２００ｃは、不正な第三者による不正な攻撃を受けたために、本来秘密に内蔵すべき鍵が暴露されており、このため、再生装置２００ｂ及び再生装置２００ｃは、無効化されている。

音楽や映画などのコンテンツの供給業者は、コンテンツサーバ装置５００及び記録装置１００を有しており、コンテンツサーバ装置５００と記録装置１０

０とは、専用回線３０を介して接続されている。

コンテンツサーバ装置５００は、コンテンツ及び前記コンテンツを暗号化する際に用いられるコンテンツ鍵を有しており、記録装置１００からの要求により、コンテンツ及び対応するコンテンツ鍵を、専用回線３０を介して、記録装置１００へ送信する。

記録装置１００は、コンテンツサーバ装置５００から、専用回線３０を介して、コンテンツ及び対応するコンテンツ鍵を受信し、受信したコンテンツとコンテンツ鍵を暗号化し、暗号化コンテンツ、暗号化コンテンツ鍵及びその他の関連する情報をして記録媒体１２０に書き込む。

暗号化コンテンツ、暗号化コンテンツ鍵及びその他の関連する情報が記録された記録媒体１２０は、販売店で売られ、利用者は、記録媒体１２０を購入する。

利用者の有する再生装置２００ａは、記録媒体１２０が装着されると、記録媒体１２０から暗号化コンテンツ、暗号化コンテンツ鍵及びその他の関連する情報を読み出し、読み出したその他の関連する情報を用いて、コンテンツの復号の可否を判断し、復号可能であると判断する場合に、暗号化コンテンツ鍵から復号コンテンツ鍵を生成し、復号コンテンツ鍵を用いて復号コンテンツを生成し、生成した復号コンテンツから映画や音楽を生成し、出力する。

１．２　コンテンツサーバ装置５００

コンテンツサーバ装置５００は、情報記憶部５０１、制御部５０２、入力部５０３、表示部５０４及び送受信部５０５から構成されている（図示していない）。

コンテンツサーバ装置５００は、具体的には、マイクロプロセッサ、ＲＯＭ、ＲＡＭ、ハードディスクユニット、通信ユニット、ディスプレィユニット、キーボード、マウスなどから構成されるコンピュータシステムである。前記ＲＡＭ又は前記ハードディスクユニットには、コンピュータプログラムが記憶されている。前記マイクロプロセッサが、前記コンピュータプログラムに従って動作することにより、コンテンツサーバ装置５００の各構成要素は、その機能を達成する。

送受信部５０５は、専用回線３０を介して、記録装置１００に接続されてお

り、記録装置１００と制御部５０２との間で情報の送受信を行う。

情報記憶部５０１は、映像情報及び音声情報が高効率で圧縮符号化されて生成されたコンテンツと当該コンテンツを暗号化する際に鍵として用いられるコンテンツ鍵との組を複数個予め記憶している。

制御部５０２は、記録装置１００から、専用回線３０及び送受信部５０５を介して、いずれかのコンテンツの取得要求を受け取る。前記取得要求を受け取ると、制御部５０２は、情報記憶部５０１から、前記取得要求により示されるコンテンツ及びコンテンツ鍵を読み出し、読み出したコンテンツ及びコンテンツ鍵を、送受信部５０５及び専用回線３０を介して、記録装置１００へ送信する。

入力部５０３は、コンテンツサーバ装置５００の操作者の指示を受け付け、受け付けた指示を制御部５０２へ出力する。

表示部５０４は、制御部５０２の制御により、様々な情報を表示する。

１．３　記録装置１００

記録装置１００は、図２に示すように、デバイス鍵格納部１０１、メディア鍵データ格納部１０２、鍵計算部１０３、鍵計算部１０４、暗号化部１０５、暗号化部１０６、秘密鍵格納部１０７、証明書格納部１０８、ＣＲＬ格納部１０９、署名生成部１１０、ドライブ部１１１、制御部１１２及び送受信部１１３から構成されている。

記録装置１００は、具体的には、コンテンツサーバ装置５００と同様に、マイクロプロセッサ、ＲＯＭ、ＲＡＭ、ハードディスクユニットなどから構成されるコンピュータシステムである。前記ＲＡＭ又は前記ハードディスクユニットには、コンピュータプログラムが記憶されている。前記マイクロプロセッサが、前記コンピュータプログラムに従って動作することにより、記録装置１００は、その機能を達成する。

（１）デバイス鍵格納部１０１

デバイス鍵格納部１０１は、外部の装置からアクセスできないように、デバイス鍵ＤＫ＿１を秘密に記憶している。デバイス鍵ＤＫ＿１は、記録装置１００に固有の鍵である。なお、本明細書において、装置ｍが保有するデバイス鍵をＤＫ＿ｍと表現している。

（２）メディア鍵データ格納部１０２

メディア鍵データ格納部１０２は、メディア鍵データＭＤＡＴＡを記憶している。メディア鍵データＭＤＡＴＡは、ｎ個の組を含み、各組は、暗号化メディア鍵及び装置番号から構成されている。各組に含まれている暗号化メディア鍵と装置番号とは対応している。ここで、ｎは、上述したように、記録装置１００及び再生装置２００ａ、２００ｂ、・・・の台数の合計値である。

ｎ個の組のうち、第１の組は、第１の暗号化メディア鍵及び装置番号「１」から構成されている。装置番号「１」は、記録装置１００を識別する識別情報である。第１の暗号化メディア鍵は、装置番号「１」により識別される装置、つまり、記録装置１００に割り当てられたデバイス鍵ＤＫ＿１を用いて、メディア鍵ＭＫに暗号化アルゴリズムＥ１を施して生成されたものである。

第１の暗号化メディア鍵＝Ｅ１（ＤＫ＿１、ＭＫ）

ここで、暗号化アルゴリズムＥ１は、一例として、ＤＥＳ（Data Encryption Standard）によるものである。また、Ｅ（Ａ、Ｂ）は、鍵Ａを用いて、平文Ｂに対して暗号化アルゴリズムＥを施して得られた暗号文を示している。

また、メディア鍵ＭＫは、記録媒体１２０に固有の鍵である。

また、ｎ個の組のうち、第２の組は、それぞれ、第２の暗号化メディア鍵及び装置番号「２」から構成されている。ここで、装置番号「２」は、再生装置２００ａを識別する。また、第２の暗号化メディア鍵は、装置番号「２」の装置、つまり、再生装置２００ａに割り当てられたデバイス鍵ＤＫ＿２を用いて、メディア鍵ＭＫに暗号化アルゴリズムＥ１を施して生成されたものである。

第２の暗号化メディア鍵＝Ｅ１（ＤＫ＿２、ＭＫ）

また、ｎ個の組のうち、第３、第４の組は、それぞれ、第３の暗号化メディア鍵及び装置番号「３」、第４の暗号化メディア鍵及び装置番号「４」から構成されている。ここで、装置番号「３」及び「４」は、それぞれ、再生装置２００ｂ、２００ｃを識別する。また、第３、第４の暗号化メディア鍵は、それぞれ、装置番号「３」、「４」により識別される装置、つまり、再生装置２００ｂ、２００ｃに割り当てられたデバイス鍵ＤＫ＿３、ＤＫ＿４を用いて、メディア鍵ＭＫの代わりに、値「０」に暗号化アルゴリズムＥ１を施して生成されたものである。

第３の暗号化メディア鍵＝Ｅ１（ＤＫ＿３、０）

第４の暗号化メディア鍵＝Ｅ１（ＤＫ＿４、０）

ここで、値「０」は、メディア鍵（ＭＫ）とは全く無関係のデータである。メディア鍵ＭＫの代わりに、値「０」を用いるのは、第３及び第４の暗号化メディア鍵に、それぞれ、対応する再生装置２００ｂ及び２００ｃが無効化されているからであり、再生装置２００ｂ及び２００ｃが無効化されていることを知るための検知情報として用いられる。

無効化された装置について、無効化された装置のデバイス鍵を用いて、メディア鍵ＭＫとは全く無関係のデータ、つまり値「０」を暗号化して暗号化メディア鍵を生成することにより、無効化された装置以外の全ての装置だけがメディア鍵ＭＫを共有できる。また、無効化された装置をこのシステムから排除することができる。

ここで、値「０」を用いるとしているが、メディア鍵ＭＫとは、全く無関係の他のデータであるとしてもよい。例えば、他の固定値である「０ｘＦＦＦＦ」、暗号化メディア鍵を生成する時点の日付や時刻を示す情報、当該無効化された装置のデバイス鍵などであるとしていもよい。

なお、装置の無効化方法は他の方法を利用してもよく、例えば、特許文献１には木構造を利用した無効化方法が開示されている。

また、ｎ個の組のうち、第５、・・・、第ｎの組は、それぞれ、第５の暗号化メディア鍵及び装置番号「５」、・・・、第ｎの暗号化メディア鍵及び装置番号「ｎ」から構成されている。ここで、装置番号「５」、・・・、「ｎ」は、それぞれ、再生装置２００ｄ、２００ｅ、・・・を識別する。また、第５、・・・、第ｎの暗号化メディア鍵は、それぞれ、装置番号「５」、・・・「ｎ」の装置、つまり、再生装置２００ｄ、２００ｅ、・・・に割り当てられたデバイス鍵ＤＫ＿５、・・・、ＤＫ＿ｎを用いて、メディア鍵ＭＫに暗号化アルゴリズムＥ１を施して生成されたものである。

第５の暗号化メディア鍵＝Ｅ１（ＤＫ＿５、ＭＫ）

・・・

第ｎの暗号化メディア鍵＝Ｅ１（ＤＫ＿ｎ、ＭＫ）

（３）鍵計算部１０３

鍵計算部１０３は、記録装置１００に割り当てられた装置番号「１」を予め記憶している。

鍵計算部１０３は、メディア鍵データ格納部１０２に記憶されているメディア鍵データＭＤＡＴＡを構成するｎ個の組から、予め記憶している装置番号「１」を含む組を探して読み出し、読み出した組から装置番号「１」に対応する暗号化メディア鍵Ｅ１（ＤＫ＿１、ＭＫ）を抽出する。

次に、鍵計算部１０３は、デバイス鍵格納部１０１からデバイス鍵ＤＫ＿１を読み出し、読み出したデバイス鍵ＤＫ＿１を用いて、抽出した暗号化メディア鍵Ｅ１（ＤＫ＿１、ＭＫ）に復号アルゴリズムＤ１を施して、メディア鍵ＭＫを生成する。

メディア鍵ＭＫ＝Ｄ１（ＤＫ＿１、（Ｅ１（ＤＫ＿１、ＭＫ））

ここで、復号アルゴリズムＤ１は、暗号化アルゴリズムＥ１を施して生成された暗号文を復号するアルゴリズムであり、一例として、ＤＥＳによるものである。また、Ｄ（Ａ、Ｂ）は、鍵Ａを用いて、暗号文Ｂに対して復号アルゴリズムＤを施して得られた復号文を示している。

次に、鍵計算部１０３は、生成したメディア鍵ＭＫを鍵計算部１０４へ出力する。

なお、図２において、記録装置１００の各構成部を示す各ブロックは、接続線により他のブロックと接続されている。ただし、一部の接続線を省略している。ここで、各接続線は、信号や情報が伝達される経路を示している。また、鍵計算部１０３を示すブロックに接続している複数の接続線のうち、接続線上に鍵マークが描かれているものは、鍵計算部１０３へ鍵としての情報が伝達される経路を示している。他の構成要素を示すブロックについても同様である。また、他の図面についても同様である。

（４）鍵計算部１０４

鍵計算部１０４は、鍵計算部１０３からメディア鍵ＭＫを受け取り、ドライブ部１１１を介して、記録媒体１２０の固有番号記録領域１２１から媒体固有番号ＭＩＤを読み出す。

次に、鍵計算部１０４は、受け取ったメディア鍵ＭＫと読み出した媒体固有番号ＭＩＤを、この順序で、結合して、結合値（ＭＫ｜｜ＭＩＤ）を生成する。

ここで、「Ａ｜｜Ｂ」は、データＡとデータＢとをこの順序でビット結合することを示す。次に、鍵計算部１０４は、生成した結合値（ＭＫ｜｜ＭＩＤ）にハッシュ関数ＳＨＡ－１を施して、ハッシュ値Ｈ＝ＳＨＡ－１（ＭＫ｜｜ＭＩＤ）を得、得られたハッシュ値Ｈを鍵暗号化鍵ＫＥＫとし、鍵暗号化鍵ＫＥＫを暗号化部１０５及び署名生成部１１０へ出力する。

ここで、ＳＨＡ－１（Ａ）は、情報Ａに対してハッシュ関数ＳＨＡ－１を施して得られたハッシュ値を示している。

なお、鍵計算部１０４は、ハッシュ関数ＳＨＡ－１を施して得られたハッシュ値を鍵暗号化鍵ＫＥＫとしているが、これに限定されることはない。得られたハッシュ値の一部分を鍵暗号化鍵ＫＥＫとしてもよい。

また、ハッシュ関数ＳＨＡ－１については、公知であるので、説明を省略する。なお、他のハッシュ関数を使用してもよい。

（５）暗号化部１０５

暗号化部１０５は、コンテンツサーバ装置５００から送受信部１１３を介して、コンテンツ鍵ＣＫを受け取り、鍵計算部１０４から鍵暗号化鍵ＫＥＫを受け取る。

次に、暗号化部１０５は、受け取った鍵暗号化鍵ＫＥＫを用いて、受け取ったコンテンツ鍵ＣＫに暗号化アルゴリズムＥ２を施して、暗号化コンテンツ鍵ＥＣＫを生成する。

暗号化コンテンツ鍵ＥＣＫ＝Ｅ２（ＫＥＫ、ＣＫ）

ここで、暗号化アルゴリズムＥ２は、一例として、ＤＥＳによるものである。

次に、暗号化部１０５は、ドライブ部１１１を介して、記録媒体１２０上に鍵記録領域１２３を確保し、次に、生成した暗号化コンテンツ鍵ＥＣＫを、ドライブ部１１１を介して、記録媒体１２０の鍵記録領域１２３へ書き込む。

（６）暗号化部１０６

暗号化部１０６は、コンテンツサーバ装置５００から送受信部１１３を介して、コンテンツ鍵ＣＫ及びコンテンツＣＮＴを受け取り、受け取ったコンテンツ鍵ＣＫを用いて、受け取ったコンテンツＣＮＴに暗号化アルゴリズムＥ３を施して暗号化コンテンツＥＣＮＴを生成する。

暗号化コンテンツＥＣＮＴ＝Ｅ３（ＣＫ、ＣＮＴ）

ここで、暗号化アルゴリズムＥ３は、一例として、ＤＥＳによるものである。

次に、暗号化部１０６は、ドライブ部１１１を介して、記録媒体１２０上にコンテンツ記録領域１２４を確保し、次に、生成した暗号化コンテンツＥＣＮＴを、ドライブ部１１１を介して、記録媒体１２０のコンテンツ記録領域１２４へ書き込む。

（７）秘密鍵格納部１０７

秘密鍵格納部１０７は、外部の装置からアクセスできないように、記録装置１００の秘密鍵ＳＫ＿１を記憶している。秘密鍵ＳＫ＿１は、公開鍵暗号方式によるものである。ここで、前記公開鍵暗号方式は、一例として、ＲＳＡ（Rivest Shamir Adleman）暗号方式である。

（８）証明書格納部１０８

証明書格納部１０８は、公開鍵証明書ＰＫＣを記憶している。公開鍵証明書ＰＫＣは、証明書識別子ＩＤ＿１、公開鍵ＰＫ＿１及び署名データＳｉｇ＿１を含んで構成される。

証明書識別子ＩＤ＿１は、公開鍵証明書ＰＫＣを一意に識別する識別情報である。公開鍵ＰＫ＿１は、秘密鍵格納部１０７に記憶されている秘密鍵ＳＫ＿１に対応する公開鍵である。また、署名データＳｉｇ＿１は、認証局ＣＡ（Certificate Authority）の秘密鍵ＳＫ＿ＣＡを用いて、証明書識別子ＩＤ＿１及び公開鍵ＰＫ＿１の結合値（ＩＤ＿１｜｜ＰＫ＿１）に対してデジタル署名Ｓｉｇを施して生成されたものである。

署名データＳｉｇ＿１＝Ｓｉｇ（ＳＫ＿ＣＡ、ＩＤ＿１｜｜ＰＫ＿１）

ここで、Ｓｉｇ（Ａ、Ｂ）は、鍵Ａを用いて、データＢに対して、デジタル署名Ｓｉｇを施して得られた署名データを示している。また、デジタル署名Ｓｉｇの一例は、ハッシュ関数ＳＨＡ－１を使ったＲＳＡを用いるデジタル署名である。

（９）ＣＲＬ格納部１０９

ＣＲＬ格納部１０９は、第１の時点における無効化された公開鍵証明書を示す公開鍵証明書無効化リスト（以下、無効化リストＣＲＬと呼ぶ。）を記録している。

無効化リストＣＲＬは、１個以上の証明書識別子と、署名データＳｉｇＩＤ

と、版数とを含んでいる。

各証明書識別子は、無効化された公開鍵証明書を識別する識別情報である。

署名データＳｉｇＩＤは、認証局ＣＡの秘密鍵ＳＫ＿ＣＡを用いて、無効化リストＣＲＬに含まれる全ての証明書識別子の結合値に対して（無効化リストＣＲＬに１個の証明書識別子が含まれている場合には、前記１個の証明書識別子に対して）、デジタル署名Ｓｉｇを施して生成されたものである。

署名データＳｉｇＩＤ＝Ｓｉｇ（ＳＫ＿ＣＡ、全ての証明書識別子の結合値）

例えば、証明書識別子ＩＤ＿３及びＩＤ＿４により識別される公開鍵証明書が無効化されている場合には、無効化リストＣＲＬは、証明書識別子ＩＤ＿３、ＩＤ＿４、署名データＳｉｇＩＤ＝Ｓｉｇ（ＳＫ＿ＣＡ、（ＩＤ＿３｜｜ＩＤ＿４））及び版数を含む。

版数は、無効化リストＣＲＬの世代を示す情報であり、無効化リストＣＲＬが前記第１の時点におけるものであることを示す。版数は、公開鍵証明書無効化リストの世代が新しいほど、大きい値をとる。

（１０）署名生成部１１０

署名生成部１１０は、秘密鍵格納部１０７から秘密鍵ＳＫ＿１を読み出し、ＣＲＬ格納部１０９から無効化リストＣＲＬを読み出し、鍵計算部１０４から鍵暗号化鍵ＫＥＫを受け取る。

次に、署名生成部１１０は、受け取った鍵暗号化鍵ＫＥＫと読み出した無効化リストＣＲＬとをこの順序で結合して結合値（ＫＥＫ｜｜ＣＲＬ）を生成し、読み出した秘密鍵ＳＫ＿１を用いて、生成した結合値（ＫＥＫ｜｜ＣＲＬ）にデジタル署名Ｓｉｇを施して署名データＳｉｇＣＲＬを生成する。

署名データＳｉｇＣＲＬ＝Ｓｉｇ（ＳＫ＿１、（ＫＥＫ｜｜ＣＲＬ））

次に、署名生成部１１０は、ドライブ部１１１を介して、記録媒体１２０上に署名記録領域１２５を確保し、次に、生成した署名データＳｉｇＣＲＬを、ドライブ部１１１を介して、記録媒体１２０の署名記録領域１２５へ書き込む。

（１１）制御部１１２

制御部１１２は、送受信部１１３を介して、コンテンツサーバ装置５００に対して、コンテンツの取得要求を送信する。

また、制御部１１２は、証明書格納部１０８から公開鍵証明書ＰＫＣを読み

出し、ドライブ部１１１を介して、記録媒体１２０上に証明書記録領域１２７を確保し、次に、読み出した公開鍵証明書ＰＫＣをドライブ部１１１を介して、記録媒体１２０の証明書記録領域１２７へ書き込む。

また、制御部１１２は、メディア鍵データ格納部１０２からメディア鍵データＭＤＡＴＡを読み出し、ドライブ部１１１を介して、記録媒体１２０上にメディア鍵データ記録領域１２２を確保し、次に、読み出したメディア鍵データＭＤＡＴＡをドライブ部１１１を介して、記録媒体１２０のメディア鍵データ記録領域１２２へ書き込む。

また、制御部１１２は、ＣＲＬ格納部１０９から無効化リストＣＲＬを読み出し、ドライブ部１１１を介して、記録媒体１２０上にＣＲＬ記録領域１２６を確保し、次に、読み出した無効化リストＣＲＬをドライブ部１１１を介して、記録媒体１２０のＣＲＬ記録領域１２６へ書き込む。

制御部１１２は、記録装置１００の操作者の操作指示によりキーボード１８０から指示情報を受け取り、指示情報に従って動作する。また、記録装置１００を構成する他の構成要素の動作を制御する。

（１２）送受信部１１３

送受信部１１３は、専用回線３０を介して、コンテンツサーバ装置５００と接続されており、コンテンツサーバ装置５００と制御部１１２との間で情報の送受信を行う。また、制御部１１２の制御の基に、コンテンツサーバ装置５００と暗号化部１０５との間で、及びコンテンツサーバ装置５００と暗号化部１０６との間で、情報の送受信を行う。

（１３）ドライブ部１１１

ドライブ部１１１は、制御部１１２の制御の基に、記録媒体１２０の固有番号記録領域１２１から媒体固有番号ＭＩＤを読み出し、読み出した媒体固有番号ＭＩＤを鍵計算部１０４へ出力する。

また、ドライブ部１１１は、制御部１１２の制御の基に、暗号化部１０５、暗号化部１０６、署名生成部１１０から各情報を受け取り、受け取った情報を書き込むための各領域を記録媒体１２０上に確保し、確保した領域に前記情報を書き込む。

また、ドライブ部１１１は、制御部１１２から情報を受け取り、受け取った

情報を書き込むための各領域を記録媒体１２０上に確保し、確保した領域に前記情報を書き込む。

（１４）キーボード１８０及びモニタ１９０

キーボード１８０は、記録装置１００の操作者の操作指示を受け付け、受け付けた操作指示に対応する指示情報を制御部１１２へ出力する。

モニタ１９０は、制御部１１２の制御により様々な情報を表示する。

１．４　記録媒体１２０

記録媒体１２０は、光ディスクメディアであり、図３に示すように、固有番号記録領域１２１と、一般領域１２９とから構成されている。

固有番号記録領域１２１には、記録媒体１２０を識別する固有の番号である媒体固有番号ＭＩＤが予め記録されている。固有番号記録領域１２１は、他の情報の書き込みや記録されている媒体固有番号ＭＩＤの書き換えができない書換不可領域である。媒体固有番号ＭＩＤは、一例として、１６進数８桁で表現されており、「０ｘ００００００００６」である。なお、本明細書において、「０ｘ」は、以降の表示が１６進数によるものであることを示している。

一般領域１２９は、他の情報の書き込みが可能な領域であり、当初、一般領域１２９には、何らの情報も書き込まれていない。

記録装置１００の上述した動作の終了後において、一般領域１２９には、図３に示すように、メディア鍵データ記録領域１２２、鍵記録領域１２３、コンテンツ記録領域１２４、署名記録領域１２５、ＣＲＬ記録領域１２６及び証明書記録領域１２７が確保される。

上述したように、第１の実施の形態では、記録装置１００及び再生装置２００ａ、２００ｂ、２００ｃ、２００ｄ、２００ｅ、・・・の台数の合計がｎ台であり、これらの装置のうち、再生装置２００ｂ及び再生装置２００ｃが無効化されており、ｎ台の装置はそれぞれ固有のデバイス鍵を１つだけ保有している、と仮定している。このような仮定に基づいて、記録媒体１２０の一般領域１２９に含まれている各領域には、具体例としての各種データが記録されている。

（メディア鍵データ記録領域１２２）

メディア鍵データ記録領域１２２には、メディア鍵データＭＤＡＴＡが記録

されている。メディア鍵データＭＤＡＴＡは、ｎ個の組から構成され、各組は、暗号化メディア鍵及び装置番号を含む。

装置番号は、装置を識別する識別情報である。

暗号化メディア鍵は、対応する装置番号「ｍ」により示される装置ｍに割り当てられたデバイス鍵ＤＫ＿ｍを用いて、メディア鍵ＭＫ又は値「０」に暗号化アルゴリズムＥ１を施して生成されたものである。ここで、装置ｍが無効化されている場合には、値「０」を用いる。また、装置ｍが無効化されていない場合には、メディア鍵ＭＫを用いる。

暗号化メディア鍵＝Ｅ１（ＤＫ＿ｍ、ＭＫ）　又は

暗号化メディア鍵＝Ｅ１（ＤＫ＿ｍ、０）

（鍵記録領域１２３）

鍵記録領域１２３には、暗号化コンテンツ鍵ＥＣＫが記録されている。暗号化コンテンツ鍵ＥＣＫは、鍵暗号化鍵ＫＥＫを用いて、コンテンツ鍵ＣＫに暗号化アルゴリズムＥ２を施して生成されたものである。

暗号化コンテンツ鍵ＥＣＫ＝Ｅ２（ＫＥＫ、ＣＫ）

ここで、鍵暗号化鍵ＫＥＫは、メディア鍵ＭＫと媒体固有番号ＭＩＤを結合した値を入力値として、ハッシュ関数の出力値を利用して算出される鍵である。

鍵暗号化鍵ＫＥＫ＝ＳＨＡ－１（ＭＫ｜｜ＭＩＤ）

（コンテンツ記録領域１２４）

コンテンツ記録領域１２４には、暗号化コンテンツＥＣＮＴが記録されている。暗号化コンテンツＥＣＮＴは、コンテンツ鍵ＣＫを用いて、コンテンツに暗号化アルゴリズムＥ３を施して生成されたものである。

暗号化コンテンツＥＣＮＴ＝Ｅ３（ＣＫ、ＣＮＴ）

（署名記録領域１２５）

署名記録領域１２５には、署名データＳｉｇＣＲＬが記録されている。

署名データＳｉｇＣＲＬは、秘密鍵ＳＫ＿１を用いて、鍵暗号化鍵ＫＥＫと無効化リストＣＲＬとの結合値（ＫＥＫ｜｜ＣＲＬ）にデジタル署名Ｓｉｇを施して生成されたものである。

署名データＳｉｇＣＲＬ＝Ｓｉｇ（ＳＫ＿１、（ＫＥＫ｜｜ＣＲＬ））

（ＣＲＬ記録領域１２６）

ＣＲＬ記録領域１２６には、無効化リストＣＲＬが記録されており、無効化リストＣＲＬには、無効化すべき証明書のＩＤが記載されている。無効化リストＣＲＬは、一例として、証明書識別子ＩＤ＿３、ＩＤ＿４、署名データＳｉｇＩＤ及び版数を含んでいる。

証明書識別子ＩＤ＿３、ＩＤ＿４は、無効化された公開鍵証明書を識別する識別情報である。

署名データＳｉｇＩＤは、認証局ＣＡの秘密鍵ＳＫ＿ＣＡを用いて、無効化リストＣＲＬに含まれる全ての証明書識別子の結合値に対して（無効化リストＣＲＬに１個の証明書識別子が含まれている場合には、前記１個の証明書識別子に対して）、デジタル署名Ｓｉｇを施して生成されたものである。

署名データＳｉｇＩＤ＝Ｓｉｇ（ＳＫ＿ＣＡ、全ての証明書識別子の結合値）

認証局ＣＡによる署名データが含まれているのは、無効化リストＣＲＬの正当性を保証するためである。

版数は、無効化リストＣＲＬの世代を示す情報である。

なお、ＣＲＬのフォーマットは公知のものであってもよいし、また、あるシステムに特化したフォーマットであってもよい。

（証明書記録領域１２７）

証明書記録領域１２７には、公開鍵証明書ＰＫＣが記録されている。公開鍵証明書ＰＫＣは、証明書識別子ＩＤ＿１、公開鍵ＰＫ＿１及び署名データＳｉｇ＿１を含んでいる。

証明書識別子ＩＤ＿１は、公開鍵証明書ＰＫＣを識別する識別情報である。

公開鍵ＰＫ＿１は、公開鍵暗号方式によるものであり、秘密鍵ＳＫ＿１に対応している。

署名データＳｉｇ＿１は、認証局ＣＡの秘密鍵ＳＫ＿ＣＡを用いて、証明書識別子ＩＤ＿１及び公開鍵ＰＫ＿１の結合値（ＩＤ＿１｜｜ＰＫ＿１）に対してデジタル署名Ｓｉｇを施して生成されたものである。

署名データＳｉｇ＿１＝Ｓｉｇ（ＳＫ＿ＣＡ、ＩＤ＿１｜｜ＰＫ＿１）

なお、認証局ＣＡによる署名データが含まれているのは、公開鍵証明書の正当性を保証するためである。

また、公開鍵証明書のフォーマットは公知のものであってもよいし、またあ

るシステムに特化したフォーマットであってもよい。

１．５　再生装置２００

再生装置２００ａ、２００ｂ、２００ｃ、・・・は、同様の構成を有しているので、ここでは、再生装置２００として説明する。

再生装置２００は、図４に示すように、デバイス鍵格納部２０１、鍵計算部２０２、鍵計算部２０３、復号部２０４、復号部２０５、ＣＡ公開鍵格納部２０６、証明書検証部２０７、ＣＲＬ格納部２０８、ＣＲＬ検証部２０９、ＣＲＬ比較更新部２１０、証明書判定部２１１、署名検証部２１２、スイッチ２１３、再生部２１４、制御部２１５、入力部２１６、表示部２１７及びドライブ部２１８から構成されている。

再生装置２００は、具体的には、コンテンツサーバ装置５００と同様に、マイクロプロセッサ、ＲＯＭ、ＲＡＭ、ハードディスクユニットなどから構成されるコンピュータシステムである。前記ＲＡＭ又は前記ハードディスクユニットには、コンピュータプログラムが記憶されている。前記マイクロプロセッサが、前記コンピュータプログラムに従って動作することにより、再生装置２００は、その機能を達成する。

（１）デバイス鍵格納部２０１

デバイス鍵格納部２０１は、外部の装置からアクセスできないように、デバイス鍵ＤＫ＿ｘを秘密に記憶している。デバイス鍵ＤＫ＿ｘは、再生装置２００に固有の鍵である。

なお、デバイス鍵格納部２０１が記憶しているデバイス鍵ＤＫ＿ｘは、再生装置２００ａ、２００ｂ、２００ｃ、２００ｄ、２００ｅ、・・・により異なる。再生装置２００ａ、２００ｂ、２００ｃ、２００ｄ、２００ｅ、・・・の各デバイス鍵格納部２０１は、それぞれ、デバイス鍵ＤＫ＿２、ＤＫ＿３、ＤＫ＿４、ＤＫ＿５、ＤＫ＿６、・・・を記憶している。

（２）鍵計算部２０２

鍵計算部２０２は、再生装置２００に割り当てられた装置番号「ｘ」を予め記憶している。なお、鍵計算部２０２が記憶している装置番号「ｘ」は、再生装置２００ａ、２００ｂ、２００ｃ、２００ｄ、２００ｅ、・・・により異なる。再生装置２００ａ、２００ｂ、２００ｃ、２００ｄ、２００ｅ、・・・の

各鍵計算部２０２は、それぞれ、装置番号「２」、「３」、「４」、「５」、「６」・・・を記憶している。

鍵計算部２０２は、記録媒体１２０のメディア鍵データ記録領域１２２から、ドライブ部２１８を介して、メディア鍵データＭＤＡＴＡを構成するｎ個の組を順に読み出し、読み出した組の中から、記憶している装置番号「ｘ」を含む組を探す。装置番号「ｘ」を含む組を発見すると、発見した組から装置番号「ｘ」に対応する暗号化メディア鍵Ｅ１（ＤＫ＿ｘ、ｙ）を抽出する。ここで、再生装置２００が、再生装置２００ｂ又は２００ｃである場合には、ｙは、値「０」である。また、再生装置２００が、再生装置２００ｂ及び２００ｃを除く他の再生装置である場合には、ｙは、メディア鍵ＭＫである。

次に、鍵計算部２０２は、デバイス鍵格納部２０１からデバイス鍵ＤＫ＿ｘを読み出し、読み出したデバイス鍵ＤＫ＿ｘを用いて、抽出した暗号化メディア鍵Ｅ１（ＤＫ＿ｘ、ｙ）に復号アルゴリズムＤ１を施して、復号メディア鍵ｙを生成する。

復号メディア鍵ｙ＝Ｄ１（ＤＫ＿ｘ、（Ｅ１（ＤＫ＿ｘ、ｙ））

ここで、復号メディア鍵ｙは、メディア鍵ＭＫ及び値「０」のいずれかである。

次に、鍵計算部２０２は、生成した復号メディア鍵ｙを鍵計算部２０３へ出力する。

（３）鍵計算部２０３

鍵計算部２０３は、鍵計算部１０４と同様に動作する。

鍵計算部２０３は、鍵計算部２０２から復号メディア鍵ｙを受け取り、ドライブ部２１８を介して、記録媒体１２０の固有番号記録領域１２１から媒体固有番号ＭＩＤを読み出す。

次に、鍵計算部２０３は、受け取った復号メディア鍵ｙと読み出した媒体固有番号ＭＩＤを、この順序で、結合して、結合値（ｙ｜｜ＭＩＤ）を生成する。次に、鍵計算部２０３は、生成した結合値（ｙ｜｜ＭＩＤ）にハッシュ関数ＳＨＡ－１を施して、ハッシュ値Ｈ’＝ＳＨＡ－１（ｙ｜｜ＭＩＤ）を得、得られたハッシュ値Ｈ’を鍵復号鍵ＫＤＫとし、鍵復号鍵ＫＤＫを復号部２０４及び署名検証部２１２へ出力する。

なお、上述したように、鍵計算部１０４が、得られたハッシュ値の一部分を鍵暗号化鍵ＫＥＫとする場合には、鍵計算部２０３も得られたハッシュ値の前記一部分と同じ部分を鍵復号鍵ＫＤＫとする。

（４）復号部２０４

復号部２０４は、記録媒体１２０の鍵記録領域１２３から、ドライブ部２１８を介して、暗号化コンテンツ鍵ＥＣＫを読み出し、鍵計算部２０３から鍵復号鍵ＫＤＫを受け取る。

次に、復号部２０４は、受け取った鍵復号鍵ＫＤＫを用いて、読み出した暗号化コンテンツ鍵ＥＣＫに復号アルゴリズムＤ２を施して、復号コンテンツ鍵ＤＣＫを生成する。

復号コンテンツ鍵ＤＣＫ＝Ｄ２（ＫＤＫ、ＥＣＫ）

ここで、復号アルゴリズムＤ２は、暗号化アルゴリズムＥ２を施して生成された暗号文を復号するアルゴリズムであり、一例として、ＤＥＳによるものである。

次に、復号部２０４は、生成した復号コンテンツ鍵ＤＣＫを復号部２０５へ出力する。

（５）復号部２０５

復号部２０５は、記録媒体１２０のコンテンツ記録領域１２４から、ドライブ部２１８を介して、暗号化コンテンツＥＣＮＴを読み出し、復号部２０４から復号コンテンツ鍵ＤＣＫを受け取る。

次に、復号部２０５は、受け取った復号コンテンツ鍵ＤＣＫを用いて、読み出した暗号化コンテンツＥＣＮＴに復号アルゴリズムＤ３を施して復号コンテンツＤＣＮＴを生成する。

復号コンテンツＤＣＮＴ＝Ｄ３（ＤＣＫ、ＥＣＮＴ）

ここで、復号アルゴリズムＤ３は、暗号化アルゴリズムＥ３を施して生成された暗号文を復号するアルゴリズムであり、一例として、ＤＥＳによるものである。

次に、復号部２０５は、生成した復号コンテンツＤＣＮＴをスイッチ２１３へ出力する。

（６）ＣＡ公開鍵格納部２０６

ＣＡ公開鍵格納部２０６は、認証局ＣＡの公開鍵ＰＫ＿ＣＡを予め記憶している。

（７）証明書検証部２０７

証明書検証部２０７は、ＣＡ公開鍵格納部２０６から公開鍵ＰＫ＿ＣＡを読み出し、記録媒体１２０の証明書記録領域１２７から、ドライブ部２１８を介して、公開鍵証明書ＰＫＣを読み出す。

次に、証明書検証部２０７は、読み出した公開鍵証明書ＰＫＣから、証明書識別子ＩＤ＿１、公開鍵ＰＫ＿１及び署名データＳｉｇ＿１を抽出し、抽出した証明書識別子ＩＤ＿１及び公開鍵ＰＫ＿１をこの順序で結合して結合値（ＩＤ＿１｜｜ＰＫ＿１）を生成する。

次に、証明書検証部２０７は、読み出した公開鍵ＰＫ＿ＣＡを用いて、抽出した署名データＳｉｇ＿１及び生成した結合値（ＩＤ＿１｜｜ＰＫ＿１）に、署名検証アルゴリズムＶｒｆｙを施して、検証結果ＲＳＬ２を得る。検証結果ＲＳＬ２は、検証成功及び検証失敗のいずれかを示す情報である。

ここで、署名検証アルゴリズムＶｒｆｙは、デジタル署名Ｓｉｇにより生成された署名データを検証するアルゴリズムである。

次に、証明書検証部２０７は、検証結果ＲＳＬ２をスイッチ２１３へ出力する。

（８）ＣＲＬ格納部２０８

ＣＲＬ格納部２０８は、第２の時点における無効化された公開鍵証明書を示す公開鍵証明書無効化リスト（以下、蓄積無効化リストＣＲＬ＿ＳＴと呼ぶ。）を記録している。

蓄積無効化リストＣＲＬ＿ＳＴは、第１の時点における無効化された公開鍵証明書を示すリストである無効化リストＣＲＬと同様に、１個以上の証明書識別子と、署名データＳｉｇＩＤと、版数とを含んでいる。

証明書識別子及び署名データＳｉｇＩＤについは、上述した通りである。

版数は、蓄積無効化リストＣＲＬ＿ＳＴの世代を示す情報であり、蓄積無効化リストＣＲＬ＿ＳＴが前記第２の時点におけるものであることを示す。版数は、公開鍵証明書無効化リストの世代が新しいほど、大きい値をとる。

（９）ＣＲＬ検証部２０９

ＣＲＬ検証部２０９は、ＣＡ公開鍵格納部２０６から公開鍵ＰＫ＿ＣＡを読み出し、記録媒体１２０のＣＲＬ記録領域１２６から、ドライブ部２１８を介して、無効化リストＣＲＬを読み出す。

次に、ＣＲＬ検証部２０９は、読み出した無効化リストＣＲＬから１個以上の証明書識別子と署名データＳｉｇＩＤとを抽出する。ここで、複数の証明書識別子が抽出された場合には、これらを無効化リストＣＲＬ内に配置されている順序で結合して結合値を生成する。また、１個の証明書識別子のみが抽出された場合には、抽出された１個の証明書識別子を前記結合値とする。

次に、ＣＲＬ検証部２０９は、読み出した公開鍵ＰＫ＿ＣＡを用いて、抽出した署名データＳｉｇＩＤと生成した前記結合値とに、署名検証アルゴリズムＶｒｆｙを施して、検証結果ＲＳＬ３を得る。検証結果ＲＳＬ３は、検証成功及び検証失敗のいずれかである。

得られた検証結果ＲＳＬ３が検証成功を示す場合には、ＣＲＬ検証部２０９は、読み出した無効化リストＣＲＬを署名検証部２１２及びＣＲＬ比較更新部２１０へ出力する。

（１０）ＣＲＬ比較更新部２１０

ＣＲＬ比較更新部２１０は、ＣＲＬ検証部２０９から無効化リストＣＲＬを受け取る。

無効化リストＣＲＬを受け取った場合に、ＣＲＬ比較更新部２１０は、受け取った無効化リストＣＲＬから版数を抽出し、ＣＲＬ格納部２０８から蓄積無効化リストＣＲＬ＿ＳＴを読み出し、読み出した蓄積無効化リストＣＲＬ＿ＳＴから版数を抽出する。次に、無効化リストＣＲＬから抽出した版数が、蓄積無効化リストＣＲＬ＿ＳＴから抽出した版数より大きいか、否かを判断する。

無効化リストＣＲＬから抽出した版数が、蓄積無効化リストＣＲＬ＿ＳＴから抽出した版数より大きいと判断した場合に、ＣＲＬ比較更新部２１０は、無効化リストＣＲＬの世代は、蓄積無効化リストＣＲＬ＿ＳＴの世代より新しいとみなし、無効化リストＣＲＬを、蓄積無効化リストＣＲＬ＿ＳＴとして、ＣＲＬ格納部２０８に上書きする。

無効化リストＣＲＬから抽出した版数が、蓄積無効化リストＣＲＬ＿ＳＴから抽出した版数より小さいか又は等しいと判断した場合に、無効化リストＣＲ

Ｌの世代は、蓄積無効化リストＣＲＬ＿ＳＴの世代より古いか又は同じとみなされ、上記の上書きは行われない。

（１１）証明書判定部２１１

証明書判定部２１１は、ＣＲＬ格納部２０８から蓄積無効化リストＣＲＬ＿ＳＴを読み出す。ここで、ＣＲＬ格納部２０８に記憶されている蓄積無効化リストＣＲＬ＿ＳＴは、ＣＲＬ比較更新部２１０により、最新のものに更新されている。また、証明書判定部２１１は、記録媒体１２０の証明書記録領域１２７から、ドライブ部２１８を介して、公開鍵証明書ＰＫＣを読み出す。

次に、証明書判定部２１１は、読み出した公開鍵証明書ＰＫＣから証明書識別子ＩＤ＿１を抽出し、抽出した証明書識別子ＩＤ＿１が、蓄積無効化リストＣＲＬ＿ＳＴに含まれているか否かを判断する。次に、判断結果ＪＤＧをスイッチ２１３へ出力する。ここで、判断結果ＪＤＧは、証明書識別子ＩＤ＿１が蓄積無効化リストＣＲＬ＿ＳＴに含まれているか否かを示す情報である。

（１２）署名検証部２１２

署名検証部２１２は、鍵計算部２０３から鍵復号鍵ＫＤＫを受け取る。また、記録媒体１２０の署名記録領域１２５から、ドライブ部２１８を介して、署名データＳｉｇＣＲＬを読み出し、記録媒体１２０の証明書記録領域１２７から、ドライブ部２１８を介して、公開鍵証明書ＰＫＣを読み出す。また、ＣＲＬ検証部２０９から無効化リストＣＲＬを受け取る。

次に、署名検証部２１２は、読み出した公開鍵証明書ＰＫＣから公開鍵ＰＫ＿１を抽出し、受け取った鍵復号鍵ＫＤＫと受け取った無効化リストＣＲＬを結合して結合値（ＫＤＫ｜｜ＣＲＬ）を生成し、抽出した公開鍵ＰＫ＿１を用いて、読み出した署名データＳｉｇＣＲＬ及び生成した結合値（ＫＤＫ｜｜ＣＲＬ）に署名検証アルゴリズムＶｒｆｙを施して、検証結果ＲＳＬ１を得る。検証結果ＲＳＬ１は、検証成功及び検証失敗のいずれかを示す情報である。

次に、署名検証部２１２は、検証結果ＲＳＬ１をスイッチ２１３へ出力する。

（１３）スイッチ２１３

スイッチ２１３は、復号部２０５から復号コンテンツＤＣＮＴを受け取る。また、証明書判定部２１１から判断結果ＪＤＧを受け取り、証明書検証部２０７から検証結果ＲＳＬ２を受け取り、署名検証部２１２から検証結果ＲＳＬ１

を受け取る。

受け取った検証結果ＲＳＬ１が検証成功を示し、かつ受け取った検証結果ＲＳＬ２が検証成功を示し、かつ受け取った判断結果ＪＤＧが、証明書識別子ＩＤ＿１が蓄積無効化リストＣＲＬ＿ＳＴに含まれていないことを示す場合に限り、スイッチ２１３は、受け取った復号コンテンツＤＣＮＴを再生部２１４へ出力する。

受け取った検証結果ＲＳＬ１が検証失敗を示し、又は受け取った検証結果ＲＳＬ２が検証失敗を示し、又は受け取った判断結果ＪＤＧが、証明書識別子ＩＤ＿１が蓄積無効化リストＣＲＬ＿ＳＴに含まれていることを示す場合に、スイッチ２１３は、受け取った復号コンテンツＤＣＮＴを再生部２１４へ出力しない。

（１４）再生部２１４

再生部２１４は、スイッチ２１３から復号コンテンツＤＣＮＴを受け取り、受け取った復号コンテンツＤＣＮＴから映像情報及び音声情報を生成し、生成した映像情報及び音声情報をアナログの映像信号及び音声信号に変換し、アナログの映像信号及び音声信号をモニタ２９０へ出力する。

（１５）制御部２１５、入力部２１６、表示部２１７、ドライブ部２１８、モニタ２９０及びリモコン２８０

制御部２１５は、再生装置２００を構成する各構成要素の動作を制御する。

リモコン２８０は、各種のボタンを備え、操作者の前記ボタンの操作に応じた操作指示情報を生成し、生成した操作指示情報を赤外線に乗せて出力する。

入力部２１６は、リモコン２８０から、操作指示情報が乗せられた赤外線を受け取り、受け取った赤外線から操作指示情報を抽出し、抽出した操作指示情報を制御部２１５へ出力する。

表示部２１７は、制御部２１５の制御の基に、様々な情報を表示する。

ドライブ部２１８は、記録媒体１２０からの情報の読み出しを行う。

モニタ２９０は、ＣＲＴ及びスピーカを備え、再生部２１４からアナログの映像信号及び音声信号を受信し、映像信号に基づいて映像を表示し、音声信号に基づいて音声を出力する。

１．６　コンテンツ供給システム１０の動作

コンテンツ供給システム１０の動作について、特に、記録装置１００による記録媒体１２０へのデータの書き込みの動作及び再生装置２００による記録媒体１２０に記録されているデータの再生の動作について、説明する。

（１）記録装置１００による書き込みの動作

記録装置１００による記録媒体１２０へのデータの書き込みの動作について、図５に示すフローチャートを用いて説明する。

鍵計算部１０３は、デバイス鍵格納部１０１及びメディア鍵データ格納部１０２から、それぞれ、デバイス鍵ＤＫ＿１及びメディア鍵データＭＤＡＴＡを読み出し（ステップＳ３０１）、次に、読み出したデバイス鍵ＤＫ＿１及びメディア鍵データＭＤＡＴＡを用いて、メディア鍵ＭＫを生成する（ステップＳ３０２）。

次に、鍵計算部１０４は、記録媒体１２０の固有番号記録領域１２１から媒体固有番号ＭＩＤを読み出し（ステップＳ３０３）、生成されたメディア鍵ＭＩＤと読み出した媒体固有番号ＭＩＤを用いて、鍵暗号化鍵ＫＥＫを算出する（ステップＳ３０４）。

次に、暗号化部１０５は、算出された鍵暗号化鍵ＫＥＫを用いて、コンテンツサーバ装置５００から取得したコンテンツ鍵ＣＫを暗号化して、暗号化コンテンツ鍵ＥＣＫを生成する（ステップＳ３０５）。

次に、暗号化部１０６は、コンテンツサーバ装置５００から取得したコンテンツ鍵ＣＫを用いて、コンテンツサーバ装置５００から取得したコンテンツＣＮＴを暗号化して暗号化コンテンツＥＣＮＴを生成する（ステップＳ３０６）。

次に、署名生成部１１０は、秘密鍵格納部１０７から秘密鍵ＳＫ＿１を読み出し（ステップＳ３０７）、読み出した秘密鍵ＳＫ＿１を用いて、鍵暗号化鍵ＫＥＫ及び無効化リストＣＲＬに対する署名データＳｉｇＣＲＬを生成する（ステップＳ３０８）。

次に、記録装置１００は、メディア鍵データＭＤＡＴＡ、暗号化コンテンツ鍵ＥＣＫ、暗号化コンテンツＥＣＮＴ、署名データＳｉｇＣＲＬ、無効化リストＣＲＬ及び公開鍵証明書ＰＫＣを、ドライブ部１１１を介して、記録媒体１２０に記録する（ステップＳ３０９）。

（２）再生装置２００による再生の動作

再生装置２００による記録媒体１２０に記録されているデータの再生の動作について、図６～図７に示すフローチャートを用いて説明する。

再生装置２００は、記録媒体１２０から、メディア鍵データＭＤＡＴＡ、媒体固有番号ＭＩＤ、暗号化コンテンツ鍵ＥＣＫ、暗号化コンテンツＥＣＮＴ、署名データＳｉｇＣＲＬ、無効化リストＣＲＬ及び公開鍵証明書ＰＫＣを読み出す（ステップＳ４０１）。

次に、鍵計算部２０２は、デバイス鍵格納部２０１からデバイス鍵ＤＫ＿ｘを読み出し（ステップＳ４０２）、読み出したメディア鍵データＭＤＡＴＡ及びデバイス鍵ＤＫ＿ｘを用いて、復号メディア鍵ｙを得る（ステップＳ４０３）。

次に、鍵計算部２０３は、読み出した媒体固有番号ＭＩＤ及び得られた復号メディア鍵ｙから鍵復号鍵ＫＤＫを算出する（ステップＳ４０４）。

次に、復号部２０４は、算出された鍵復号鍵ＫＤＫを用いて、読み出した暗号化コンテンツ鍵ＥＣＫを復号して復号コンテンツ鍵ＤＣＫを得る（ステップＳ４０５）。

次に、復号部２０５は、読み出した暗号化コンテンツＥＣＮＴを、得られた復号コンテンツ鍵ＤＣＫを用いて、復号して、復号コンテンツＤＣＮＴを得る（ステップＳ４０６）。

次に、証明書検証部２０７は、ＣＡ公開鍵格納部２０６から認証局ＣＡの公開鍵ＰＫ＿ＣＡを読み出し（ステップＳ４０７）、読み出した認証局ＣＡの公開鍵ＰＫ＿ＣＡを用いて、読み出した公開鍵証明書ＰＫＣの正当性を検証する（ステップＳ４０８）。

公開鍵証明書ＰＫＣの正当性の検証に失敗した場合には（ステップＳ４０９）、ステップＳ４２２へ制御が移る。公開鍵証明書ＰＫＣの正当性の検証に成功した場合には（ステップＳ４０９）、ＣＲＬ検証部２０９は、認証局ＣＡの公開鍵ＰＫ＿ＣＡを用いて、読み出した無効化リストＣＲＬの正当性を検証する（ステップＳ４１０）。

無効化リストＣＲＬの正当性の検証に失敗した場合には（ステップＳ４１１）、ステップＳ４２２へ制御が移る。無効化リストＣＲＬの正当性の検証に成功した場合には（ステップＳ４１１）、ＣＲＬ比較更新部２１０は、ＣＲＬ格納部２０８から蓄積無効化リストＣＲＬ＿ＳＴを読み出し（ステップＳ４１２）、

記録媒体１２０から読み出した無効化リストＣＲＬと、ＣＲＬ格納部２０８から読み出した蓄積無効化リストＣＲＬ＿ＳＴとの新旧を比較する（ステップＳ４１３）。

ＣＲＬ比較更新部２１０は、上記の比較の結果、無効化リストＣＲＬの方が、蓄積無効化リストＣＲＬ＿ＳＴより新しいと判断される場合に（ステップＳ４１４）、新しいと判断した無効化リストＣＲＬを蓄積無効化リストＣＲＬ＿ＳＴととして、ＣＲＬ格納部２０８に上書きする（ステップＳ４１５）。無効化リストＣＲＬの方が、蓄積無効化リストＣＲＬ＿ＳＴより古いと判断される場合（ステップＳ４１４）、ステップＳ４１６へ制御が移る。

次に、証明書判定部２１１は、ＣＲＬ格納部２０８から蓄積無効化リストＣＲＬ＿ＳＴを読み出し（ステップＳ４１６）、読み出した公開鍵証明書ＰＫＣから抽出した証明書識別子ＩＤ＿１が、蓄積無効化リストＣＲＬ＿ＳＴに含まれているか否かを判断することにより、読み出した蓄積無効化リストＣＲＬ＿ＳＴに公開鍵証明書ＰＫＣが登録されているか否かを判定する（ステップＳ４１７）。

登録されていると判定された場合（ステップＳ４１８）、ステップＳ４２２へ制御が移る。登録されていないと判定された場合（ステップＳ４１８）、署名検証部２１２は、鍵復号鍵ＫＤＫ、公開鍵証明書ＰＫＣ及び無効化リストＣＲＬを用いて、署名データＳｉｇＣＲＬの正当性を検証する（ステップＳ４１９）。

署名データＳｉｇＣＲＬの正当性の検証に失敗した場合（ステップＳ４２０）、スイッチ２１３は、開かれ、コンテンツは再生されず（ステップＳ４２２）、再生装置２００の再生動作が終了する。

一方、署名データＳｉｇＣＲＬの正当性の検証に成功した場合（ステップＳ４２０）、スイッチ２１３は、閉じられ、復号コンテンツＤＣＮＴを再生部２１４へ出力し、再生部２１４は、復号コンテンツＤＣＮＴを再生し（ステップＳ４２１）、再生装置２００の再生動作が終了する。

１．７　その他の変形例

（１）第１の実施の形態では、記録媒体を介して、無効化リストＣＲＬを伝播する仕組みを実現するために、記録装置が、無効化リストＣＲＬを署名対象

として署名データＳｉｇＣＲＬを生成し、生成した署名データＳｉｇＣＲＬを記録媒体に書き込むとしているが、本発明は、この構成に限定されるものではない。

例えば、記録装置は、無効化リストＣＲＬのハッシュ値を算出して、そのハッシュ値に対して署名データを生成するとしてもよい。

署名データ＝Ｓｉｇ（ＳＫ＿１、ＨＡＳＨ（ＣＲＬ））

ここで、ＨＡＳＨ（Ａ）は、データＡに対してハッシュ関数ＨＡＳＨを施して得られたハッシュ値である。

また、記録装置は、無効化リストＣＲＬのハッシュ値を算出して、そのハッシュ値とメディア鍵ＭＫをＸＯＲ（排他的論理和）演算し、その演算結果に対して署名データを生成するとしてもよい。

署名データ＝Ｓｉｇ（ＳＫ＿１、（ＨＡＳＨ（ＣＲＬ））ＸＯＲ（ＭＫ））

このように、記録装置は、無効化リストＣＲＬ及びコンテンツに対して署名データを生成したり、無効化リストＣＲＬ及び各種鍵データに対して署名データを生成したりし、生成した署名データを記録媒体に書き込むことにより、記録媒体上の無効化リストＣＲＬの改ざんや削除を防止することができる。

また、これらの場合に、再生装置は、それぞれ、対応するデータを用いて、署名検証を行う。

（２）第１の実施の形態では、外部から取得する無効化リストＣＲＬ及び内部に記憶している無効化リストＣＲＬの新旧を比較する際に、バージョン番号を比較するとしているが、本発明は、この構成に限定されるものではない。

例えば、無効化リストＣＲＬが更新されるにつれて、無効化リストＣＲＬのサイズが単調に増加すると仮定できれば、ＣＲＬのサイズが大きい方を新しいと判断してもよい。

同様に、無効化リストＣＲＬが更新されるにつれて、無効化される装置の数が単調に増加すると仮定できれば、無効化する装置の台数の比較により、無効化台数が多い方を新しいと判断してもよい。

以上のように、ＣＲＬから新旧比較できる情報を得ることができる構成であれば、如何なる構成であってもよい。

（３）別の記録媒体を介して、メディア鍵データの最新版が、記録装置に対

して、伝播する構成であってもよい。

前記別の記録媒体には、最新版のメディア鍵データが記録されている。

記録装置は、内部に予めメディア鍵データを保有している。メディア鍵データが記録されている前記別の記録媒体が装着されると、記録装置は、自身が保有しているメディア鍵データと、記録媒体に記録されているメディア鍵データとの新旧を比較し、自身が保有するメディア鍵データよりも、記録媒体に記録されているメディア鍵データの方が、新しければ、自ら保有しているメディア鍵データに代えて、記録媒体に記録されているメディア鍵データを内部に書き込む。

ここで、各メディア鍵データには、その世代を示すバージョン番号が付与されており、記録装置は、各バージョン番号を用いて、各メディア鍵データの新旧を比較する。

また、メディア鍵データから算出されるメディア鍵の一部はバージョン番号であり、残りの部分は、乱数を用いて生成されるとしてもよい。記録装置は、各メディア鍵データからメディア鍵の一部のバージョン番号を抽出し、抽出した各バージョン番号を用いて、各メディア鍵データの新旧を比較する。

また、メディア鍵データにおいて無効化されている装置の台数、つまり、メディア鍵ＭＫに代えて値「０」が暗号化の対象となっている暗号化メディア鍵の数は、メディア鍵データの更新につれて、単調に増加すると仮定し、記録装置は、メディア鍵データに含まれている無効化されている装置の台数を用いて、各メディア鍵データの新旧を比較するとしてもよい。

また、各メディア鍵データには、当該メディア鍵データが生成された時刻情報（年月日時分秒）が付与されており、記録装置は、各時刻情報を用いて、各メディア鍵データの新旧を比較するとしてもよい。

以上のように、メディア鍵データの新旧を正しく比較できる構成であれば、如何なる構成であってもよい。

また、各メディア鍵データには、改ざん防止のための認証局ＣＡの署名が付与されているとしてもよい。記録装置は、署名を検証することにより、メディア鍵データの正当性を確認する。

（４）メディア鍵データ及び暗号化コンテンツなどが予め記録されている記

録媒体に対して、さらに、別の暗号化コンテンツを追加して書き込む場合に、記録装置は、自身が保有するメディア鍵データに基づいて、又は前記記録媒体に記録されているメディア鍵データに基づいて、外部（例えば、コンテンツサーバ装置）から取得したコンテンツを暗号化して、別の暗号化コンテンツを生成し、生成した別の暗号化コンテンツを前記記録媒体に書き込むとしてもよい。

この場合、前記記録媒体上には、複数のメディア鍵データ、複数の公開鍵証明書、複数の無効化リストＣＲＬが存在する場合がある。

また、記録装置は、前記記録媒体上のメディア鍵データと、記録装置が保有しているメディア鍵データとの新旧を比較し、記録装置が保有しているメディア鍵データの方が新しければ、前記記録媒体に記録されている暗号化コンテンツを復号して、復号コンテンツを生成し、生成した復号コンテンツを自身が保有する新しいメディア鍵に基づいて暗号化して、再暗号化コンテンツを生成し、生成した再暗号化コンテンツを前記記録媒体に書き込むとしてもよい。このとき、前記記録媒体に記録されている暗号化コンテンツを削除するとしてもよい。

（５）第１の実施の形態では、鍵暗号化鍵ＫＥＫに対して、デジタル署名を施して署名データを生成するとしているが、本発明はこの構成に限定されるものではない。

例えば、コンテンツＣＮＴ全体のハッシュ値に対して、デジタル署名を施して署名データを生成するとしてもよい。

署名データ＝Ｓｉｇ（ＳＫ＿１、（ＨＡＳＨ（ＣＮＴ））

即ち、署名は、コンテンツを記録した記録装置の正当性の確認が目的であるため、署名の対象となるデータは、コンテンツに関連する情報や暗号化の際に用いる鍵に関連する情報であれば、如何なる情報であってもよい。

（６）第１の実施の形態では、記録装置１００は、図２に示すように、デバイス鍵格納部１０１、メディア鍵データ格納部１０２、鍵計算部１０３、鍵計算部１０４、暗号化部１０５、暗号化部１０６、秘密鍵格納部１０７、証明書格納部１０８、ＣＲＬ格納部１０９、署名生成部１１０、ドライブ部１１１、制御部１１２及び送受信部１１３から構成される一体の装置であるとしているが、本発明は、この構成には限定されない。

例えば、デバイス鍵格納部１０１、メディア鍵データ格納部１０２、鍵計算

部１０３、鍵計算部１０４、暗号化部１０５、暗号化部１０６、秘密鍵格納部１０７、証明書格納部１０８、ＣＲＬ格納部１０９、署名生成部１１０、ドライブ部１１１及び制御部１１２の一部が一体となったドライブ装置から構成され、制御部１１２の他の一部及び送受信部１１３が一体となった処理装置から構成されているとしてもよい。この構成では、記録媒体に対するデータの読出／書込及び暗号処理を行うドライブ装置と、他の処理を行う処理装置とに分離している。

また、デバイス鍵格納部１０１、メディア鍵データ格納部１０２、秘密鍵格納部１０７、証明書格納部１０８及びＣＲＬ格納部１０９は、外部の記憶装置の記憶領域上に構成されているとしてもよい。ここで、前記外部の記憶装置の一例は、可搬型のセキュアなメモリカードである。

また、第１の実施の形態では、再生装置２００は、図４に示すように、デバイス鍵格納部２０１、鍵計算部２０２、鍵計算部２０３、復号部２０４、復号部２０５、ＣＡ公開鍵格納部２０６、証明書検証部２０７、ＣＲＬ格納部２０８、ＣＲＬ検証部２０９、ＣＲＬ比較更新部２１０、証明書判定部２１１、署名検証部２１２、スイッチ２１３、再生部２１４、制御部２１５、入力部２１６、表示部２１７及びドライブ部２１８から構成される一体の装置であるとしているが、本発明は、この構成には限定されない。

デバイス鍵格納部２０１、鍵計算部２０２、鍵計算部２０３、復号部２０４、復号部２０５、ＣＡ公開鍵格納部２０６、証明書検証部２０７、ＣＲＬ格納部２０８、ＣＲＬ検証部２０９、ＣＲＬ比較更新部２１０、証明書判定部２１１、署名検証部２１２、スイッチ２１３及びドライブ部２１８から構成される一体となったドライブ装置から構成され、再生部２１４、制御部２１５、入力部２１６及び表示部２１７から構成される一体となった処理装置から構成されているとしてもよい。この構成では、記録媒体に対するデータの読出／書込及び暗号処理を行うドライブ装置と、他の処理を行う処理装置とに分離している。

また、デバイス鍵格納部２０１、ＣＡ公開鍵格納部２０６及びＣＲＬ格納部２０８は、外部の記憶装置の記憶領域上に構成されているとしてもよい。ここで、前記外部の記憶装置の一例は、可搬型のセキュアなメモリカードである。

以上のように、記録装置及び再生装置は、それぞれ、一体の装置ではなく、

データ読出／書込装置及び処理装置の別々の構成であってもよい。この場合、データ読出／書込装置で暗号処理を行としてもよいし、処理装置で暗号処理を行うとしてもよい。

（7）第１の実施の形態では、メディア鍵データＭＤＡＴＡ、暗号化コンテンツ鍵ＥＣＫ、暗号化コンテンツＥＣＮＴ、署名データＳｉｇＣＲＬ、無効化リストＣＲＬ及び公開鍵証明書ＰＫＣを全て同一の記録媒体に記録するとしているが、本発明は、この構成に限定されるものではない。

例えば、記録装置１００は、署名データＳｉｇＣＲＬ、無効化リストＣＲＬ、公開鍵証明書ＰＫＣなどのデータの一部を、記録媒体１２０とは別の記録媒体に記録し、記録媒体１２０及びこの別の記録媒体が配布されるとしてもよい。

また、記録装置１００は、インターネットを代表とするネットワークに接続されており、これらのデータの一部を、ネットワークを介して配布するとしてもよい。再生装置２００も、ネットワークに接続されており、記録装置１００から、ネットワークを介して、これらのデータの一部を取得する。

以上のように、メディア鍵データＭＤＡＴＡ、暗号化コンテンツ鍵ＥＣＫ、暗号化コンテンツＥＣＮＴ、署名データＳｉｇＣＲＬ、無効化リストＣＲＬ及び公開鍵証明書ＰＫＣが、１個以上の記録媒体に記録されて配布され、又は、１個以上の記録媒体に記録されかつネットワークを介して配布されるとしてもよい。

（8）第１の実施の形態では、デバイス鍵に基づいて、コンテンツを暗号化し、また暗号化コンテンツを復号しているが、本発明は、この構成に限定されるものではない。

例えば、記録装置及び再生装置が利用条件を取得しており、その利用条件に基づいて記録及び再生を制御する構成であってもよい。ここで、利用条件とは、コンテンツに付随する管理情報であり、例えば、コンテンツの記録及び再生を許可する日付、時間、又は回数である。

（9）第１の実施の形態では、再生装置がＣＲＬ格納部から無効化リストＣＲＬを読み出して新旧比較を行い、新しい無効化リストＣＲＬをＣＲＬ格納部に格納し、公開鍵証明書の登録有無の確認時に再度、無効化リストＣＲＬを読み出すとしているが、本発明は、この構成に限定されるものではない。

例えば、再生装置は、無効化リストＣＲＬの新旧比較を行うことなく、また、新しいと判断した無効化リストＣＲＬをＣＲＬ格納部に格納することなく、公開鍵証明書の無効化リストＣＲＬでの登録の有無を判定した後に、記録媒体１２０から読み出した無効化リストＣＲＬをＣＲＬ格納部へ格納するとしてもよい。

また、署名検証、ＣＲＬ検証、公開鍵証明書判定の順序も、第１の実施の形態に記載の如く限定されず、再生装置は、種々の順序により、署名検証、ＣＲＬ検証、公開鍵証明書判定を行い、コンテンツの再生を制御するとしてもよい。

（１０）記録装置及び再生装置が電子透かしを生成して埋め込む電子透かし処理部を備える構成であってもよい。

例えば、記録装置がその装置を特定する装置ＩＤを記憶しており、コンテンツの記録媒体への記録時に、コンテンツに対して、その装置ＩＤを電子透かしとして埋め込むとしてもよい。

このとき、装置ＩＤが電子透かしとして埋め込まれたコンテンツが不正流出した場合に、コンテンツから、埋め込まれた装置ＩＤを抽出することにより、そのコンテンツを記録した記録装置を特定することができる。

また、同様に再生装置が再生時に、自身の装置ＩＤを電子透かしとして、記録媒体上のコンテンツに埋め込む構成であってもよい。このとき、装置ＩＤが埋め込まれたコンテンツが不正流出した場合に、コンテンツから、埋め込まれた装置ＩＤを抽出することにより、そのコンテンツを再生した再生装置を特定することができる。

（１１）コンテンツ供給システムは、暴露されたデバイス鍵を持つ不正装置が発見された場合に、内部に格納されているデバイス鍵を特定することができるデバイス鍵発見装置を含むとしてもよい。この不正装置は、再生装置２００と同じ構成を有している。

デバイス鍵発見装置は、図８に示すように、ｎ枚の記録媒体ＭＤ１、ＭＤ２、ＭＤ３、・・・、ＭＤｎを生成する。なお、図８では、メディア鍵データ以外の他のデータについては、図示を省略している。

記録媒体ＭＤ１、ＭＤ２、ＭＤ３、・・・、ＭＤｎは、以下の点を除いて、第３に示す記録媒体１２０と同じ内容のデータを記録している。

（ａ）記録媒体ＭＤ１、ＭＤ２、ＭＤ３、・・・、ＭＤｎに記録されている無効化リストＣＲＬに登録されている無効化された公開鍵証明書はない。つまり、無効化リストＣＲＬは、公開鍵証明書の識別子を含んでいない。

（ｂ）記録媒体ＭＤ１、ＭＤ２、ＭＤ３、・・・、ＭＤｎに記録されている各メディア鍵データは、記録媒体１２０に記録されているメディア鍵データとは異なるものである。記録媒体ＭＤ１、ＭＤ２、ＭＤ３、・・・、ＭＤｎに記録されている各メディア鍵データの一例を図８に示す。

（ｂ－１）記録媒体ＭＤ１に記録されているメディア鍵データは、ｎ個の組から構成される。各組は、暗号化メディア鍵と装置番号とを含む。装置番号については、第１の実施の形態において説明した通りである。

第１の暗号化メディア鍵は、デバイス鍵ＤＫ＿１を用いて、メディア鍵ＭＫに暗号化アルゴリズムＥ１を施して生成されたものである。

第２、第３、・・・、第ｎの暗号化メディア鍵は、それぞれ、デバイス鍵ＤＫ＿２、ＤＫ＿３、・・・、ＤＫ＿ｎを用いて、値「０」に暗号化アルゴリズムＥ１を施して生成されたものである。

（ｂ－２）記録媒体ＭＤ２に記録されているメディア鍵データは、ｎ個の組から構成される。各組は、暗号化メディア鍵と装置番号とを含む。装置番号については、第１の実施の形態において説明した通りである。

第１の暗号化メディア鍵は、デバイス鍵ＤＫ＿１を用いて、値「０」に暗号化アルゴリズムＥ１を施して生成されたものである。

第２の暗号化メディア鍵は、デバイス鍵ＤＫ＿２を用いて、メディア鍵ＭＫに暗号化アルゴリズムＥ１を施して生成されたものである。

第３、・・・、第ｎの暗号化メディア鍵は、それぞれ、デバイス鍵ＤＫ＿３、・・・、ＤＫ＿ｎを用いて、値「０」に暗号化アルゴリズムＥ１を施して生成されたものである。

（ｂ－３）記録媒体ＭＤ３、・・・、ＭＤｎについて、上記と同様である。

整数ｉ（１≦ｉ≦ｎ）について、記録媒体ＭＤｉに記録されているメディア鍵データは、ｎ個の組から構成される。各組は、暗号化メディア鍵と装置番号とを含む。装置番号については、第１の実施の形態において説明した通りである。

第ｉの暗号化メディア鍵は、デバイス鍵ＤＫ＿ｉを用いて、値「０」に暗号化アルゴリズムＥ１を施して生成されたものである。

その他の暗号化メディア鍵は、対応するデバイス鍵を用いて、メディア鍵ＭＫに暗号化アルゴリズムＥ１を施して生成されたものである。

次に、操作者は、記録媒体ＭＤ１、ＭＤ２、ＭＤ３、・・・、ＭＤｎを一枚ずつ順に、不正装置に装着し、コンテンツの再生を不正装置に対して指示する。

こうして、ｎ枚の記録媒体が不正装置により試される。

不正装置によりコンテンツが正しく再生された場合に、装着された記録媒体により、不正装置が内蔵するであろうデバイス鍵を特定することができる。

例えば、記録媒体ＭＤ１が装着された場合に、不正装置によりコンテンツが正しく再生されたのであれば、不正装置が内蔵するデバイス鍵は、ＤＫ＿１である。

一般化して言うと、記録媒体ＭＤｉが装着された場合に、不正装置によりコンテンツが正しく再生されたのであれば、不正装置が内蔵するデバイス鍵は、ＤＫ＿ｉである。

不正装置は、再生装置２００と同じ構成を有しており、図６～図７に示すように動作するので、記録媒体ＭＤ１、ＭＤ２、ＭＤ３、・・・、ＭＤｎのいずれか一枚が装着された場合に限り、コンテンツを正しく再生する。

（１２）第１の実施の形態では、署名生成アルゴリズムとして、署名対象データにその署名を付与する付録型署名を用いるとしているが、本発明は、この構成に限定されるものではない。

例えば、メッセージ付録型署名ではなく、メッセージ回復型署名を使用するとしてもよい。なお、メッセージ回復型署名については、特許文献３に開示されている。

メッセージ回復型署名では、署名者が、生成する署名に秘密情報を埋め込むことが可能であり、検証者が、署名検証後にその秘密情報を得ることが可能である。この特徴を利用して、記録装置は、秘密情報と鍵データ（例えばコンテンツ鍵）とにＸＯＲ演算（排他的論理和）を施し、演算結果に対して、メッセージ回復型署名を施して署名データを生成する。このとき、再生装置は、署名検証をし、検証が成功した場合に、前記演算結果を得、内蔵している秘密情報

と演算結果に対して、ＸＯＲ演算（排他的論理和）を施して、鍵データ（例えばコンテンツ鍵）を得る。

なお、秘密情報と鍵データとの間の演算は、ＸＯＲ演算に限定する必要はなく、加算演算や、両データを結合したデータを入力値として、ハッシュ関数の出力値を利用する構成であってもよい。

また、秘密情報を作用させる情報は、コンテンツ鍵である必要はなく、鍵暗号化鍵などの他の鍵であってもよい。

以上のように、署名検証することで得られる秘密情報を獲得しない限り、コンテンツの再生が行えない構成であれば如何なる構成であってもよい。このように、メッセージ回復型署名を利用することで、コンテンツの再生には署名検証が必須となる。

（１３）第１の実施の形態では、コンテンツ鍵及びコンテンツは、記録装置の外部から取得するとしているが、本発明は、この構成に限定されるものではない。

例えば、コンテンツ記録装置内部に、予めコンテンツ鍵及びコンテンツを対応付けて格納しているとしてもよい。また、コンテンツ鍵を、利用の都度、記録装置内部で生成するとしてもよい。

（１４）第１の実施の形態では、種々の検証、並びに判定結果に基づいて制御されるスイッチ２１３は、復号部２０５と再生部２１４との間に備えられ、再生部２１４に対して復号コンテンツの出力を行うか否かを制御するとしているが、本発明は、この構成に限定されるものではない。

例えば、スイッチ２１３は、復号部２０４と復号部２０５との間に備えられ、復号部２０５に対して復号コンテンツ鍵の出力を行うか否かを制御するとしてもよい。

また、スイッチ２１３は、鍵計算部２０３と復号部２０４との間に備えられ、復号部２０４に対して、鍵復号鍵ＫＤＫの出力を行うか否かを制御するとしてもよい。

このように、各検証の結果に基づき、最終的なコンテンツの再生を制御できる構成であれば如何なる構成であってもよい。さらに、スイッチ２１３は物理的なスイッチである必要はなく、再生制御を行える構成であれば、ソフトウェ

アによる構成であってもよい。

また、鍵計算部２０２は、生成した復号メディア鍵ｙが、検知情報である値「０」であるか否かを判断し、復号メディア鍵ｙが値「０」であると判断する場合に、スイッチ２１３に対して、復号コンテンツＤＣＮＴを再生部２１４へ出力しないように指示するとしてもよい。

また、鍵計算部２０２は、復号メディア鍵ｙが値「０」であると判断する場合に、鍵計算部２０３、復号部２０４、復号部２０５の全て又はいずれかに対して、鍵復号鍵の生成、復号コンテンツ鍵の生成、復号コンテンツの生成を行わないように指示するとしてもよい。

また、鍵計算部２０２は、復号メディア鍵ｙが値「０」であると判断する場合に、制御部２１５に対して、復号メディア鍵ｙが値「０」である旨のメッセージを通知し、制御部２１５は、前記メッセージを受け取ると、再生装置２００を構成する他の構成要素に対して、暗号化コンテンツの復号及び再生を中止するように指示するとしてもよい。

（１５）第１の実施の形態では、メディア鍵、鍵暗号化鍵及びコンテンツ鍵の３階層から暗号化システムを採用しているが、本発明は、この構成に限定されるものではない。

例えば、コンテンツ鍵を省き、鍵暗号化鍵で直接コンテンツを暗号化する構成であってもよい。あるいは、新たな鍵を導入してその階層を１階層増やす構成であってもよい。

（１６）記録装置又は再生装置は、インターネットに代表されるネットワークを介して、メディア鍵データ及び無効化リストＣＲＬの最新版を取得し、内蔵するデータを更新する構成であってもよい。

（１７）第１の実施の形態では、記録装置が無効化リストＣＲＬを記録媒体に記録するとしているが、本発明は、この構成に限定されるものではない。

例えば、再生装置は、無効化リストＣＲＬを、ネットワークを介して取得するものとして、記録装置は、ＣＲＬを記録媒体に記録しない構成であってもよい。

（１８）第１の実施の形態では、記録装置が、記録媒体に記録するコンテンツ又はコンテンツに関連する情報に対して署名データを生成し、生成した署名

データを記録媒体に記録するとしているが、本発明は、この構成に限定されるものではない。

例えば、記録装置は、署名生成を行わないとしてもよい。このとき、記録装置は、自身が保有するメディア鍵データ及び媒体固有番号に基づいてコンテンツを暗号化して、暗号化に使用したメディア鍵データと、暗号化されたコンテンツを記録媒体に記録するとしてもよい。このとき、再生装置は、記録媒体からメディア鍵データ、媒体固有番号、及び暗号化コンテンツを読み出し、メディア鍵データ、及び媒体固有番号に基づいてコンテンツを復号する。

（１９）第１の実施の形態では、記録装置は、メディア鍵及び媒体固有番号から鍵暗号化鍵を生成することにより、メディアバインドを実現しているが、本発明は、この構成に限定されるものではない。

例えば、記録装置は、メディア鍵及び媒体固有番号に基づいて認証子を生成して、生成した認証子を記録媒体に記録することにより、メディアバインドを実現するとしてもよい。このとき、再生装置は、同じく、メディア鍵及び媒体固有番号から認証子を生成し、記録媒体に記録された認証子と、生成した認証子が一致するか否かを判定してコンテンツの再生を制御する。

上記の認証子の生成方法は、一例として、次の通りである。

メディア鍵、媒体固有番号及び暗号化コンテンツ鍵を結合した値に、ハッシュ関数を施し、得られたハッシュ値、又はハッシュ値の特定の一部を認証子とする。

（２０）第１の実施の形態では、１枚の記録媒体は、１個のコンテンツ供給システムのみに対応しているが、本発明は、この構成に限定されるものではない。

複数のコンテンツ供給システムが存在し、例えば、１のコンテンツ供給システムは、映画のコンテンツを供給するシステムである。別のコンテンツ供給システムは、コンピュータソフトウェアを供給するシステムである。さらに別のコンテンツ供給システムは、音楽を供給するシステムである。このように、供給されるコンテンツの種類により、異なるコンテンツ供給システムが用いられる。

また、例えば、１のコンテンツ供給システムは、映画供給業者Ａにより、映

画のコンテンツを供給するシステムである。別のコンテンツ供給システムは、映画供給業者Ｂにより、映画のコンテンツを供給するシステムである。さらに別のコンテンツ供給システムは、映画供給業者Ｃにより、映画のコンテンツを供給するシステムである。このように、コンテンツの供給者により、異なるコンテンツ供給システムが用いられることもある。

ここでは、１枚の記録媒体が、異なる複数のコンテンツ供給システムにおいて利用される仕組みについて、説明する。

記録媒体の書き換え不可領域には、記録媒体に固有の媒体固有番号に加え、鍵の無効化データが予め記録されている。このとき、第１のコンテンツ供給システムは、予め書き換え不可領域に記録されている鍵の無効化データを使用することにより、著作物保護の仕組みを実現する。また、第２のコンテンツ供給システムは、第１の実施の形態に示した構成で、著作物保護の仕組みを実現する。

図９に、前記記録媒体に記録されるデータの一例を示す。

記録媒体７００には、書き換え不可領域７１０と、書き換え可能領域７２０が存在し、書き換え不可領域７１０には、第１のコンテンツ供給システム用の鍵無効化データ記録領域７１１と、固有番号記録領域７１２が存在する。また、書き換え可能領域７２０には、第２のコンテンツ供給システム用の鍵無効化データ記録領域７２１と、第１の暗号化コンテンツ鍵記録領域７２２と、第２の暗号化コンテンツ鍵記録領域７２３と、その他の暗号化コンテンツ記録領域（図示していない）とが存在する。

ここで、第２のコンテンツ供給システム用の鍵無効化データ記録領域７２１は、第１の実施の形態におけるメディア鍵データ記録領域１２２に相当する。さらに、第１の暗号化コンテンツ鍵記録領域７２２には、第１のコンテンツ供給システム用の鍵無効化データに基づいて暗号化されたデータが記録され、同様に、第２の暗号化コンテンツ鍵記録領域７２３には、第２のコンテンツ供給システム用の鍵無効化データに基づいて暗号化されたデータが記録される。

このように、１つの記録媒体が複数のコンテンツ供給システムをサポートする場合、媒体固有番号はシステムごとに複数存在する必要はなく、記録媒体に唯一でよく、各コンテンツ供給システムが同一の媒体固有番号、あるいはその

一部分を共通に使用する構成であってもよい。

ここで、媒体固有番号の一部分を使用するとは、例えば１２８ビットの媒体固有番号が存在した場合に、上位３２ビットは使用せず、下位９６ビットを媒体固有番号として使用したり、媒体固有番号の上位３２ビットをオール０に置き換え、１２８ビットの媒体固有番号として使用したりすることを意味する。

以上のように、記録媒体に予め記録されている媒体固有番号を複数のコンテンツ供給システムで共通に使用することにより、既に市販され利用されている媒体固有番号のみを記録した記録媒体においても、著作物の著作権を保護することができるシステムの実現が可能となる。また、システムごとに媒体固有番号を記録する必要がないことにより、書き換え不可領域の容量削減も可能である。

以上のように、本発明は、少なくとも第１及び第２のコンテンツ供給システムに対して著作物保護の仕組みを提供する著作物保護システムである。

記録媒体は、読出専用の書換不可領域と、読出し及び書込みの可能な書換可能領域とを備え、前記書換不可領域には、当該記録媒体に固有の媒体固有番号と、第１のコンテンツ供給システム用に鍵無効化データとが予め記録されている。

第１のコンテンツ供給システムは、前記記録媒体にコンテンツを暗号化して書き込む記録装置と、前記記録媒体に記録されている暗号化コンテンツの復号を試みる複数の再生装置とから構成されている。前記複数の再生装置のうちいずれか１台以上は、無効化されている。前記記録媒体の前記書換不可領域に記録されている前記鍵無効化データは、前記無効化された再生装置の鍵を示している。

前記記録装置は、前記書換不可領域に記録されている前記無効化データを用いて、コンテンツを暗号化する暗号化部と、生成した暗号化コンテンツを前記記録媒体の前記書換可能領域に書き込む書込部とを備える。

前記再生装置は、前記記録媒体の前記書換不可領域に記録されている前記鍵無効化データと、前記記録媒体に記録されている前記暗号化コンテンツを読み出す読出部と、読み出した前記鍵無効化データを用いて、前記暗号化コンテンツの復号を許可するか否かを判断する判断部と、復号が許可されない場合に、

前記暗号化コンテンツの復号を禁止し、復号が許可される場合に、前記暗号化コンテンツを復号して、復号コンテンツを生成する復号部とを備える。

また、第２のコンテンツ供給システムは、前記記録媒体にコンテンツを暗号化して書き込む記録装置と、前記記録媒体に記録されている暗号化コンテンツの復号を試みる複数の再生装置とから構成されている。前記複数の再生装置のうちいずれか１台以上は、無効化されている。

前記記録装置は、無効化されていない各再生装置についてメディア鍵が、無効化された各再生装置について所定の検知情報が、それぞれ、当該再生装置のデバイス鍵を用いて、暗号化されて生成された複数の暗号化メディア鍵から構成されるメディア鍵データを記憶している記憶部と、前記記録媒体の前記書換不可領域から前記媒体固有番号を読み出す読出部と、読み出した前記媒体固有番号及び前記メディア鍵に基づいて、暗号化鍵を生成する生成部と、生成された前記暗号化鍵に基づいて、デジタルデータであるコンテンツを暗号化して暗号化コンテンツを生成する暗号化部と、前記記憶部から前記メディア鍵データを読み出す読出部と、読み出された前記メディア鍵データ及び生成された前記暗号化コンテンツを前記記録媒体の前記書換可能領域に書き込む書込部とを備える。

各再生装置は、前記記録媒体の前記書換可能領域に書き込まれたメディア鍵データから当該再生装置に対応する暗号化メディア鍵を読み出す読出部と、当該再生装置のデバイス鍵を用いて、読み出された前記暗号化メディア鍵を復号して復号メディア鍵を生成する復号部と、生成された復号メディア鍵が、前記検知情報であるか否かを判断し、前記検知情報である場合に、前記記録媒体に記録されている暗号化コンテンツの復号を禁止し、前記検知情報でない場合に、暗号化コンテンツの復号を許可する制御部と、復号が許可された場合に、前記記録媒体から前記暗号化コンテンツを読み出し、生成された復号メディア鍵に基づいて、読み出した前記暗号化コンテンツを復号して復号コンテンツを生成する復号部とを備える。

１．８　まとめ

以上説明したように、本発明は、コンテンツを暗号化して記録する記録装置と、前記暗号化コンテンツを記録する記録媒体と、前記記録媒体から暗号化コ

ンテンツを読み出して復号する再生装置からなる著作権保護システムである。

前記記録装置は、特定装置が保有する鍵を無効化するための無効化データを保持して、前記無効化データに基づいて前記コンテンツを暗号化して、前記記録媒体に、前記無効化データ、並びに前記暗号化コンテンツを記録して、さらに、前記コンテンツ、あるいは前記コンテンツの暗号化に関連するデータに対して署名を生成して、前記生成した署名を前記記録媒体に記録する。

前記記録媒体は、ユーザにより書き換えできない領域に、前記記録媒体を一意に識別する識別番号を記録して、さらに、前記無効化データ、前記暗号化コンテンツ、並びに前記署名を記録する。

前記再生装置は、前記記録媒体から、前記無効化データ、前記暗号化コンテンツ、並びに前記署名を読み出して、前記無効化データに基づいて前記コンテンツを復号して、前記署名の正当性を検証した結果に基づいて、前記復号したコンテンツの再生を制御するとしてもよい。

ここで、前記著作権保護システムにおいて、前記記録媒体は、前記無効化データ、並びに前記暗号化コンテンツを記録して、前記署名は、前記記録媒体とは異なる記録媒体、あるいは通信媒体を介して配布されるとしてもよい。

ここで、前記著作権保護システムにおいて、前記記録装置は、２つ以上の装置の組み合わせで処理を行い、前記装置ごとに処理を分担するとしてもよい。

ここで、前記著作権保護システムにおいて、前記再生装置は、２つ以上の装置の組み合わせで処理を行い、前記装置ごとに処理を分担するとしてもよい。

ここで、前記著作権保護システムにおいて、前記記録装置は、コンテンツの利用条件に基づいてコンテンツを記録するとしてもよい。

ここで、前記著作権保護システムにおいて、前記再生装置は、コンテンツの利用条件に基づいてコンテンツを再生するとしてもよい。

ここで、前記著作権保護システムにおいて、前記記録装置は、前記記録装置を一意に識別する装置特定番号を保持して、コンテンツの記録に際して、前記装置特定番号を電子透かしとして前記コンテンツに埋め込むとしてもよい。

ここで、前記著作権保護システムにおいて、前記再生装置は、前記再生装置を一意に識別する装置特定番号を保持して、コンテンツの再生に際して、前記装置特定番号を電子透かしとして前記コンテンツに埋め込むとしてもよい。

ここで、前記著作権保護システムにおいて、不正装置が発見された際に、前記不正装置が保有する鍵の種類を判定する鍵発見装置を含むとしてもよい。

また、本発明は、コンテンツを暗号化して記録する記録装置である。前記記録装置は、特定装置が保有する鍵を無効化するための無効化データを保持して、前記無効化データに基づいて前記コンテンツを暗号化して、記録媒体に、前記無効化データ、並びに前記暗号化コンテンツを記録して、さらに、前記コンテンツ、あるいは前記コンテンツの暗号化に関連するデータに対して署名を生成して、前記生成した署名を前記記録媒体に記録する。

ここで、前記記録装置は、前記無効化データに加えて、前記記録媒体を一意に識別する識別番号に基づいて前記コンテンツを暗号化するとしてもよい。

ここで、前記記録装置は、前記署名の生成に使用した秘密鍵に対応する公開鍵を前記記録媒体に記録するとしてもよい。

ここで、前記記録装置は、公開鍵の無効化リストを署名対象として署名生成を行うとしてもよい。

ここで、前記記録装置は、前記コンテンツを記録する記録媒体に無効化データが存在する場合に、前記記録装置が保有する無効化データと、前記記録媒体に存在する無効化データの新旧を比較して、新しい無効化データを保有するとしてもよい。

ここで、前記記録装置は、前記無効化データの新旧の比較を、無効化データのサイズの比較で行い、サイズの大きい無効化データを新しいと判断するとしてもよい。

ここで、前記記録装置は、前記無効化データの新旧の比較を、無効化している鍵数の比較で行い、無効化している鍵数が多い無効化データを新しいと判断するとしてもよい。

ここで、前記記録装置は、前記無効化データの新旧の比較を、無効化データの生成日、あるいはバージョン番号の比較で行い、前記生成日、あるいは前記バージョン番号は、改ざんから保護されているとしてもよい。

ここで、前記記録装置は、前記コンテンツを記録する記録媒体に無効化データ、並びに暗号化コンテンツが存在して、かつ、前記記録装置が保有する無効化データが、前記記録媒体に記録されている無効化データと比較して新しい場

合に、前記記録媒体に記録された前記暗号化コンテンツを、同様に、前記記録媒体に記録された無効化データに基づいて一旦復号して、前記記録装置が保有する無効化データに基づいて再暗号化するとしてもよい。

ここで、前記記録装置は、前記記録装置内部で秘密情報を生成して、前記秘密情報と前記無効化データに基づいて前記コンテンツを暗号化して、前記秘密情報を署名に埋め込む情報として署名を生成するとしてもよい。

また、本発明は、記録媒体から暗号化コンテンツを読み出して復号する再生装置である。前記再生装置は、前記記録媒体から、無効化データ、前記暗号化コンテンツ、並びに署名を読み出して、前記無効化データに基づいて前記コンテンツを復号して、前記署名の正当性を検証した結果に基づいて、前記復号したコンテンツの再生を制御する。

ここで、前記再生装置は、前記無効化データに加えて、前記記録媒体を一意に識別する識別番号に基づいて前記暗号化コンテンツを復号するとしてもよい。

ここで、前記再生装置は、公開鍵の無効化リストを保有して、前記無効化リストを使用して、前記署名の正当性の検証に使用する公開鍵が、前記無効化リストに登録されているか否かを判断して、前記判断した結果に基づいて、前記復号したコンテンツの再生を制御するとしてもよい。

ここで、前記再生装置は、前記記録媒体に前記無効化リストが存在する場合に、前記再生装置が保有する無効化リストと、前記記録媒体に存在する無効化リストの新旧を比較して、新しい無効化リストを保有するとしてもよい。

ここで、前記再生装置は、前記無効化リストの新旧の比較を、無効化リストのサイズの比較で行い、サイズの大きい無効化リストを新しいと判断するとしてもよい。

ここで、前記再生装置は、前記無効化リストの新旧の比較を、無効化している公開鍵数の比較で行い、無効化している公開鍵数が多い無効化リストを新しいと判断するとしてもよい。

ここで、前記再生装置は、前記署名の正当性の検証を行うことにより秘密情報を獲得して、前記獲得した秘密情報、並びに無効化データに基づいて、前記暗号化コンテンツを復号するとしてもよい。

また、本発明は、暗号化コンテンツを記録する記録媒体である。前記記録媒

体は、ユーザにより書き換えできない領域に、前記記録媒体を一意に識別する識別番号を記録して、さらに、無効化データ、暗号化コンテンツ、並びに署名を記録している。

ここで、前記記録媒体は、前記無効化データ、並びに識別番号に基づいて暗号化されたコンテンツを記録しているとしてもよい。

ここで、前記記録媒体は、前記署名の生成に使用した秘密鍵に対応する公開鍵を記録しているとしてもよい。

ここで、前記記録媒体は、２つ以上の記録装置により記録された場合に、２つ以上の無効化データ、並びに２つ以上の公開鍵を記録しているとしてもよい。

以上、説明したように、第１の実施の形態においては、記録装置が、メディア鍵データから算出されるメディア鍵に基づいてコンテンツを暗号化し、かつ記録装置自身の公開鍵証明書及び生成した署名を合わせて記録媒体に記録することで、記録媒体の書き換え不可領域に鍵無効化情報が記録されていない記録媒体であっても、鍵無効化及びメディアバインドを実現して、不正装置を使ったコンテンツの記録又は再生による著作物侵害の防止を実現することができきる。

具体的には、正規の記録装置及び不正な再生装置が存在する場合、正規の記録装置は、不正な再生装置の無効化を示すメディア鍵データに基づいてコンテンツを暗号化して記録媒体に記録する。その記録媒体を挿入した不正な再生装置は、記録されているメディア鍵データからはメディア鍵を復号することができないため、不正な再生装置によるコンテンツの再生を防止できる。

また、不正な記録装置及び正規の再生装置が存在する場合、不正な記録装置は、自身が無効化されていない古いメディア鍵データに基づいてコンテンツを暗号化して記録媒体に記録する。このとき、記録装置自身の公開鍵証明書及び生成した署名データも記録する。その記録媒体を挿入した正規の再生装置は、記録されているメディア鍵データからメディア鍵を復号することができる。しかし、コンテンツの再生前に記録装置の公開鍵証明書が無効化リストＣＲＬに登録されているか否かを判断するため、無効化リストＣＲＬに登録されている不正な記録装置により記録されたコンテンツであれば、その再生を止めることができる。

２．第２の実施の形態

本発明に係る別の実施の形態としてのコンテンツ供給システム２０について説明する。

２．１　コンテンツ供給システム２０の構成

コンテンツ供給システム２０は、コンテンツ供給システム１０と類似した構成を有しており、図１０に示すように、配信局装置１４００、コンテンツサーバ装置１５００、記録装置１１００及び再生装置１２００ａ、１２００ｂ、１２００ｃ、１２００ｄ、１２００ｅ、・・・から構成されている。

第１の実施の形態と同様に、再生装置のうちの一部は、無効化されている。

２．２　配信局装置１４００

配信局装置１４００は、情報記憶部１４０１、制御部１４０２、入力部１４０３、表示部１４０４及び送受信部１４０５から構成されている（図示していない）。

配信局装置１４００は、具体的には、第１の実施の形態のコンテンツサーバ装置５００と同様に、マイクロプロセッサ、ＲＯＭ、ＲＡＭ、ハードディスクユニット、通信ユニット、ディスプレィユニット、キーボード、マウスなどから構成されるコンピュータシステムである。前記ＲＡＭ又は前記ハードディスクユニットには、コンピュータプログラムが記憶されている。前記マイクロプロセッサが、前記コンピュータプログラムに従って動作することにより、配信局装置１４００の各構成要素は、その機能を達成する。

送受信部１４０５は、インターネット４０を介して、記録装置１１００と接続されており、記録装置１１００と制御部１４０２との間で情報の送受信を行う。

情報記憶部１４０１は、鍵無効化データＲＤＡＴＡとバージョン番号ＶＲとを対応付けて予め記憶している。

鍵無効化データＲＤＡＴＡは、第１の実施の形態のメディア鍵データＭＤＡＴＡと同一である。ここでは、詳細の説明を省略する。

バージョン番号ＶＲは、当該バージョン番号ＶＲに対応する鍵無効化データＲＤＡＴＡの世代を示す情報である。

制御部１４０２は、記録装置１１００から、インターネット４０及び送受信

部１４０５を介して、鍵無効化データＲＤＡＴＡの取得要求を受け取る。前記取得要求を受け取ると、制御部１４０２は、情報記憶部１４０１から、鍵無効化データＲＤＡＴＡとバージョン番号ＶＲとを読み出し、読み出した鍵無効化データＲＤＡＴＡとバージョン番号ＶＲとを、送受信部１４０５及びインターネット４０を介して、記録装置１１００へ送信する。

入力部１４０３は、配信局装置１４００の操作者の指示を受け付け、受け付けた指示を制御部１４０２へ出力する。

表示部１４０４は、制御部１４０２の制御により、様々な情報を表示する。

２．３　コンテンツサーバ装置１５００

コンテンツサーバ装置１５００は、第１の実施の形態のコンテンツサーバ装置５００と同一の構成を有している。ここでは、説明を省略する。

２．４　記録装置１１００

記録装置１１００は、図１１に示すように、デバイス鍵格納部１１０１、無効化データ格納部１１０２、鍵計算部１１０３、暗号化部１１０５、暗号化部１１０６、認証子生成部１１０４、割当部１１０７、比較部１１０８、制御部１１０９、ドライブ部１１１０及び送受信部１１１１から構成されている。

記録装置１１００は、具体的には、記録装置１００と同様に、マイクロプロセッサ、ＲＯＭ、ＲＡＭ、ハードディスクユニットなどから構成されるコンピュータシステムである。前記ＲＡＭ又は前記ハードディスクユニットには、コンピュータプログラムが記憶されている。前記マイクロプロセッサが、前記コンピュータプログラムに従って動作することにより、記録装置１１００は、その機能を達成する。

（１）デバイス鍵格納部１１０１

デバイス鍵格納部１１０１は、外部の装置からアクセスできないように、デバイス鍵ＤＫ＿１を秘密に記憶している。デバイス鍵ＤＫ＿１は、記録装置１１００に固有の鍵である。

（２）無効化データ格納部１１０２

無効化データ格納部１１０２は、配信局装置１４００から取得した鍵無効化データＲＤＡＴＡとバージョン番号ＶＲとを記憶するための領域を有している。

（３）鍵計算部１１０３

鍵計算部１１０３は、第１の実施の形態の鍵計算部１０３と同様の構成を有している。

鍵計算部１１０３は、無効化データ格納部１１０２から鍵無効化データＲＤＡＴＡを読み出し、デバイス鍵格納部１１０１からデバイス鍵ＤＫ＿１を読み出す。次に、鍵計算部１０３と同様に、読み出したデバイス鍵ＤＫ＿１を用いて、読み出した鍵無効化データＲＤＡＴＡに復号アルゴリズムＤ１を施してメディア鍵ＭＫを生成し、生成したメディア鍵ＭＫを認証子生成部１１０４及び暗号化部１１０５へ出力する。

（４）暗号化部１１０５

暗号化部１１０５は、コンテンツサーバ装置１５００から、送受信部１１１１を介して、コンテンツ鍵ＣＫを受け取り、鍵計算部１１０３からメディア鍵ＭＫを受け取る。

次に、暗号化部１１０５は、受け取ったメディア鍵ＭＫを用いて、受け取ったコンテンツ鍵ＣＫに暗号化アルゴリズムＥ２を施して、暗号化コンテンツ鍵ＥＣＫを生成する。

暗号化コンテンツ鍵ＥＣＫ＝Ｅ２（ＭＫ、ＣＫ）

次に、暗号化部１１０５は、ドライブ部１１１０を介して、記録媒体１３００上の暗号化コンテンツファイル１３２０内に鍵記録部１３２３を確保し、次に、生成した暗号化コンテンツ鍵ＥＣＫを、ドライブ部１１１０を介して、鍵記録部１３２３へ書き込む。

また、暗号化部１１０５は、生成した暗号化コンテンツ鍵ＥＣＫを認証子生成部１１０４へ出力する。

（５）暗号化部１１０６

暗号化部１１０６は、コンテンツサーバ装置１５００から、送受信部１１１１を介して、コンテンツ鍵ＣＫ及びコンテンツＣＮＴを受け取り、受け取ったコンテンツ鍵ＣＫを用いて、受け取ったコンテンツＣＮＴに暗号化アルゴリズムＥ３を施して暗号化コンテンツＥＣＮＴを生成する。

暗号化コンテンツＥＣＮＴ＝Ｅ３（ＣＫ、ＣＮＴ）

次に、暗号化部１１０６は、ドライブ部１１１０を介して、記録媒体１３００上の暗号化コンテンツファイル１３２０内にコンテンツ記録部１３２４を確

保し、次に、生成した暗号化コンテンツＥＣＮＴを、ドライブ部１１１０を介して、コンテンツ記録領域１２４へ書き込む。

（６）認証子生成部１１０４

認証子生成部１１０４は、鍵計算部１１０３からメディア鍵ＭＫを受け取り、暗号化部１１０５から暗号化コンテンツ鍵ＥＣＫを受け取り、記録媒体１３００の固有番号記録領域１３０１から媒体固有番号ＭＩＤを読み出す。

次に、認証子生成部１１０４は、受け取ったメディア鍵ＭＫと、読み出した媒体固有番号ＭＩＤと、受け取った暗号化コンテンツ鍵ＥＣＫとをこの順序で結合して、結合データを生成し、生成した結合データに一方向性関数Ｆを施して、認証子ＭＡＣ（Message Authentication Code）を生成する。

ＭＡＣ＝Ｆ（ＭＫ｜｜ＥＣＫ｜｜ＭＩＤ）

ここで、Ｆ（Ａ）は、データＡに対して一方向性関数Ｆを施して得られた値を示している。また、一方向性関数Ｆの一例は、ハッシュ関数ＳＨＡ－１である。

次に、認証子生成部１１０４は、ドライブ部１１１０を介して、記録媒体１３００上の暗号化コンテンツファイル１３２０内に認証子記録部１３２２を確保し、生成した認証子ＭＡＣを、ドライブ部１１１０を介して、認証子記録部１３２２に書き込む。

このようにして生成された認証子ＭＡＣは、再生装置１２００においてコンテンツの正当性を判定する際に用いられる。

（７）割当部１１０７

割当部１１０７は、記録媒体１３００に記録する鍵無効化データＲＤＡＴＡに対して、記録媒体１３００においてその鍵無効化データＲＤＡＴＡを一意に識別する鍵無効化データ識別子ＲＩＤを生成する。次に、ドライブ部１１１０を介して、記録媒体１３００上の暗号化コンテンツファイル１３２０内に識別子記録部１３２１を確保し、生成した鍵無効化データ識別子ＲＩＤを、ドライブ部１１１０を介して、識別子記録部１３２１に書き込む。

なお、割当部１１０７による鍵無効化データ識別子ＲＩＤの具体的な割当方法については後述する。

（８）比較部１１０８

比較部１１０８は、制御部１１０９の指示により、ドライブ部１１１０を介して、記録媒体１３００に鍵無効化データファイルが存在するか否かを確認する。次に、ドライブ部１１１０から鍵無効化データファイルが存在するか否かを示す存否情報を受け取る。

受け取った存否情報が、記録媒体１３００に鍵無効化データファイルが存在しないことを示す場合には、比較部１１０８は、割当部１１０７に対して、鍵無効化データ識別子ＲＩＤの生成を指示し、また、ドライブ部１１１０に対して、無効化データ格納部１１０２に記録されている鍵無効化データＲＤＡＴＡと、そのバージョン番号ＶＲと、割当部１１０７により生成された鍵無効化データ識別子ＲＩＤとから構成される鍵無効化データファイルを記録媒体１３００に書き込むように指示する。

前記存否情報が、記録媒体１３００に鍵無効化データファイルが存在することを示す場合には、比較部１１０８は、ドライブ部１１１０を介して、記録媒体１３００上の各鍵無効化データファイルから鍵無効化データＦＤＡＴＡに含まれているバージョン番号ＶＦを読み出す。この場合に、１個以上のバージョン番号ＶＦが読み出される。また、無効化データ格納部１１０２から鍵無効化データＲＤＡＴＡに対応するバージョン番号ＶＲを読み出す。

次に、比較部１１０８は、読み出したバージョン番号ＶＲと同じ内容のバージョン番号が、読み出した１個以上のバージョン番号ＶＦの中に存在するか否かを判断し、存在しないと判断する場合に、上記と同様に、割当部１１０７に対して、鍵無効化データ識別子ＲＩＤの生成を指示し、また、ドライブ部１１１０に対して、無効化データ格納部１１０２に記録されている鍵無効化データＲＤＡＴＡと、そのバージョン番号ＶＲと、割当部１１０７により生成された鍵無効化データ識別子ＲＩＤとから構成される鍵無効化データファイルを記録媒体１３００に書き込むように指示する。

存在すると判断する場合に、比較部１１０８は、読み出したバージョン番号ＶＲと同じ内容のバージョン番号が存在することを示す情報を制御部１１０９へ出力する。

（９）制御部１１０９

制御部１１０９は、送受信部１１１１及びインターネット４０を介して、配

信局装置１４００に対して、鍵無効化データＲＤＡＴＡの取得要求を送信する。また、制御部１１０９は、送受信部１１１１を介して、コンテンツサーバ装置１５００に対して、コンテンツの取得要求を送信する。

制御部１１０９は、比較部１１０８に対して、記録媒体１３００に鍵無効化データファイルが存在するか否かを確認するように指示する。

比較部１１０８からバージョン番号ＶＲと同じ内容のバージョン番号が存在することを示す情報を受け取った場合には、ドライブ部１１１０に対して、記録媒体１３００上において、バージョン番号ＶＲと同じ内容のバージョン番号を含む鍵無効化データファイルから鍵無効化データ識別子ＲＩＤを読み出すように指示し、ドライブ部１１１０から鍵無効化データ識別子ＲＩＤを受け取る。

次に、制御部１１０９は、鍵計算部１１０３に対して、デバイス鍵ＤＫ＿１と鍵無効化データＲＤＡＴＡとを読み出してメディア鍵ＭＫを生成するように指示し、暗号化部１１０５に対して、コンテンツ鍵ＣＫを暗号化するように指示し、認証子生成部１１０４に対して、媒体固有番号ＭＩＤを読み出して、認証子ＭＡＣを生成するように指示し、暗号化部１１０６に対して、コンテンツＣＮＴを暗号化するにように指示し、次に、ドライブ部１１１０に対して、記録媒体１３００上に暗号化コンテンツファイルを確保するように指示し、認証子生成部１１０４、暗号化部１１０５及び暗号化部１１０６に対して、それぞれ、生成された認証子ＭＡＣと、生成された暗号化コンテンツ鍵ＥＣＫと、生成された暗号化コンテンツＥＣＮＴとを記録媒体１３００上の暗号化コンテンツファイル内に書き込むように指示する。また、ドライブ部１１１０に対して、記録媒体１３００上の暗号化コンテンツファイル内に、識別子記録部１３０３を確保するように指示し、割当部１１０７により生成された又はドライブ部１１１０から受け取った鍵無効化データ識別子ＲＩＤを識別子記録部１３０３に書き込むように指示する。

（１０）送受信部１１１１

送受信部１１１１は、インターネット４０を介して、配信局装置１４００と接続されている。また、専用回線３０を介して、コンテンツサーバ装置１５００と接続されている。

送受信部１１１１は、配信局装置１４００から、インターネット４０を介し

て、鍵無効化データＲＤＡＴＡとバージョン番号ＶＲとを受信する。鍵無効化データＲＤＡＴＡとバージョン番号ＶＲとを受信すると、受信した鍵無効化データＲＤＡＴＡ及びバージョン番号ＶＲを、対応付けて、無効化データ格納部１１０２へ書き込む。

また、送受信部１１１１は、専用回線３０を介して、コンテンツサーバ装置１５００から、コンテンツ鍵ＣＫ及びコンテンツＣＮＴを受信し、受信したコンテンツ鍵ＣＫ及びコンテンツＣＮＴを暗号化部１１０６へ出力し、受信したコンテンツ鍵ＣＫを暗号化部１１０５へ出力する。

（１１）ドライブ部１１１０

ドライブ部１１１０は、記録装置１１００を構成する各構成要素の指示により、記録媒体１３００から情報を読み出し、読み出した情報を当該構成要素へ出力する。

また、ドライブ部１１１０は、記録装置１１００を構成する各構成要素の指示により、記録媒体１３００に各領域を確保し、また、各構成要素から情報を受け取り、確保した領域に受け取った前記情報を書き込む。

（１２）キーボード１１８０及びモニタ１１９０

キーボード１１８０は、記録装置１１００の操作者の操作指示を受け付け、受け付けた操作指示に対応する指示情報を制御部１１０９へ出力する。

モニタ１１９０は、制御部１１０９の制御により様々な情報を表示する。

２．５　記録媒体１３００

記録媒体１３００は、記録媒体１２０と同様に、光ディスクメディアであり、図１２に示すように、書換不可領域１３０８と、書換可能領域１３０９とから構成されている。

書換不可領域１３０８は、図１２に示すように、固有番号記録領域１３０１を有している。記録媒体１３００の製造時に、固有番号記録領域１３０１には、記録媒体１３００に固有の媒体固有番号ＭＩＤが記録される。このとき、書換可能領域１３０９には、何も記録されていない。この図では、媒体固有番号ＭＩＤは１６進数８桁で表現されており、具体的には、「５」である。

その後、上述したように、記録装置１１００により記録媒体１３００上に情報が書き込まれると、書換可能領域１３０９には、記録装置１１００により記

録領域１３０５と記録領域１３０６とが確保され、記録領域１３０５には、１個以上の鍵無効化データファイルが記録され、記録領域１３０６には、１個以上の暗号化コンテンツファイルが記録される。

一例として、図１２に示すように、記録領域１３０５には、鍵無効化データファイル１３１０が記録され、記録領域１３０６には、暗号化コンテンツファイル１３２０が記録される。なお、図１２に示す記録媒体１３００には、一例として、１個の鍵無効化データファイルと１個の暗号化コンテンツファイルとが記録されているが、１個以上の鍵無効化データファイルと１個以上の暗号化コンテンツファイルとが記録媒体上に記録されることもある。

鍵無効化データファイル１３１０は、図１２に示すように、版数記録部１３１１、識別子記録部１３１２及びデータ記録部１３１３から構成されている。

版数記録部１３１１には、鍵無効化データＲＤＡＴＡの世代を示すバージョン番号が記録されており、識別子記録部１３１２には、記録装置１１００の割当部１１０７により割り当てられた鍵無効化データ識別子ＲＩＤが記録されており、データ記録部１３１３には、鍵無効化データＲＤＡＴＡが記録されている。

ここで、バージョン番号、鍵無効化データ識別子ＲＩＤ及び鍵無効化データＲＤＡＴＡについては、上述した通りである。

図１２において、バージョン番号は、１６進数４桁で表現されており、具体的には、「３」である。第２の実施の形態では、配信局装置１４００から、鍵無効化データのバージョン番号が割当てられる。

図１２において、鍵無効化データ識別子は、１６進数４桁で表現されており、鍵無効化データ識別子ＲＩＤは、具体的には、「１」である。

また、暗号化コンテンツファイル１３２０は、図１２に示すように、識別子記録部１３２１、認証子記録部１３２２、鍵記録部１３２３及びコンテンツ記録部１３２４から構成されている。また、暗号化コンテンツファイル１３２０には、当該ファイルに含まれている暗号化コンテンツを識別するコンテンツ番号が付加されている（図示していない）。

識別子記録部１３２１には、鍵無効化データ識別子ＲＩＤが記録されている。鍵無効化データ識別子ＲＩＤは、コンテンツの暗号化において使用された鍵無

効化データに対して、記録装置１１００の割当部１１０７により割り当てられたものである。

認証子記録部１３２２には、認証子ＭＡＣが記録されている。認証子ＭＡＣは、記録装置１１００の認証子生成部１１０４により生成されたものである。

鍵記録部１３２３には、記録装置１１００の暗号化部１１０５により、生成された暗号化コンテンツ鍵ＥＣＫが記録されている。

コンテンツ記録部１３２４には、記録装置１１００の暗号化部１１０６により、生成された暗号化コンテンツＥＣＮＴが記録されている。

２．６　再生装置１２００

再生装置１２００ａ、１２００ｂ、１２００ｃ、・・・は、同様の構成を有しているので、ここでは、再生装置１２００として説明する。

再生装置１２００は、図１３に示すように、デバイス鍵格納部１２０１、鍵計算部１２０２、認証子生成部１２０３、復号部１２０４、復号部１２０５、比較部１２０６、指定受付部１２０７、取得部１２０８、検索部１２０９、スイッチ１２１１、ドライブ部１２１３、再生部１２１４、制御部１２１５、入力部１２１６及び表示部１２１７から構成されている。

再生装置１２００は、具体的には、再生装置２００と同様に、マイクロプロセッサ、ＲＯＭ、ＲＡＭ、ハードディスクユニットなどから構成されるコンピュータシステムである。前記ＲＡＭ又は前記ハードディスクユニットには、コンピュータプログラムが記憶されている。前記マイクロプロセッサが、前記コンピュータプログラムに従って動作することにより、再生装置１２００は、その機能を達成する。

（１）指定受付部１２０７

指定受付部１２０７は、利用者から、リモコン１２８０及び入力部１２１６を介して、再生すべきコンテンツの指定を受け付け、指定を受け付けたコンテンツを識別するコンテンツ番号を取得部１２０８及び認証子生成部１２０３へ出力する。

（２）取得部１２０８

取得部１２０８は、指定受付部１２０７からコンテンツ番号を受け取り、ドライブ部１２１３を介して、記録媒体１３００の記録領域１３０５より、受け

取ったコンテンツ番号が付加された暗号化コンテンツファイル１３２０を見出し、見出した暗号化コンテンツファイル１３２０の識別子記録部１３２１から、鍵無効化データ識別子ＲＩＤを読み出す。次に、読み出した鍵無効化データ識別子ＲＩＤを検索部１２０９へ出力する。

（３）検索部１２０９

検索部１２０９は、取得部１２０８から鍵無効化データ識別子ＲＩＤを受け取る。鍵無効化データ識別子ＲＩＤを受け取ると、ドライブ部１２１３を介して、記録媒体１３００の記録領域１３０５に記録された１個以上の鍵無効化データファイルから、受け取った鍵無効化データ識別子ＲＩＤと同じ内容の鍵無効化データ識別子を識別子記録部に含む鍵無効化データファイルを検索し、検索された鍵無効化データファイルのデータ記録部より、鍵無効化データＲＤＡＴＡを読み出す。

次に、検索部１２０９は、読み出した鍵無効化データＲＤＡＴＡを鍵計算部１２０２へ出力する。

（４）デバイス鍵格納部１２０１

デバイス鍵格納部１２０１は、デバイス鍵格納部２０１と同様に、外部の装置からアクセスできないように、デバイス鍵ＤＫ＿ｘを秘密に記憶している。デバイス鍵ＤＫ＿ｘは、再生装置１２００に固有の鍵である。

（５）鍵計算部１２０２

鍵計算部１２０２は、検索部１２０９から鍵無効化データＲＤＡＴＡを受け取り、デバイス鍵格納部１２０１からデバイス鍵ＤＫ＿ｘを読み出す。

次に、鍵計算部１２０２は、鍵計算部２０２と同様にして、読み出したデバイス鍵ＤＫ＿ｘを用いて、受け取った鍵無効化データＲＤＡＴＡに復号アルゴリズムＤ１を施して、復号メディア鍵ｙを生成する。

ここで、復号メディア鍵ｙは、メディア鍵ＭＫ及び値「０」のいずれかである。

次に、鍵計算部１２０２は、生成した復号メディア鍵ｙを認証子生成部１２０３及びスイッチ１２１１へ出力する。

（６）認証子生成部１２０３

認証子生成部１２０３は、鍵計算部１２０２から復号メディア鍵ｙを受け取

り、ドライブ部１２１３を介して、記録媒体１３００の固有番号記録領域１３０１から媒体固有番号ＭＩＤを読み出す。また、指定受付部１２０７からコンテンツ番号を受け取り、ドライブ部１２１３を介して、記録媒体１３００上において、受け取った前記コンテンツ番号が付加された暗号化コンテンツファイル１３２０を特定し、特定された暗号化コンテンツファイル１３２０の鍵記録部１３２３から暗号化コンテンツ鍵ＥＣＫを読み出す。

次に、受け取った復号メディア鍵ｙと、読み出した暗号化コンテンツ鍵ＥＣＫと、読み出した媒体固有番号ＭＩＤとをこの順序で結合して、結合データを生成し、生成した結合データに一方向性関数Ｆを施して、復号認証子ＤＭＡＣを生成する。

ＤＭＡＣ＝Ｆ（ｙ｜｜ＥＣＫ｜｜ＭＩＤ）

次に、認証子生成部１２０３は、生成した復号認証子ＤＭＡＣを比較部１２０６へ出力する。

（７）比較部１２０６

比較部１２０６は、認証子生成部１２０３から復号認証子ＤＭＡＣを受け取る。また、比較部１２０６は、指定受付部１２０７からコンテンツ番号を受け取り、ドライブ部１２１３を介して、記録媒体１３００上において、受け取った前記コンテンツ番号が付加された暗号化コンテンツファイル１３２０を特定し、特定された暗号化コンテンツファイル１３２０の認証子記録部１３２２に記録されている認証子ＭＡＣを読み出す。

次に、比較部１２０６は、受け取った復号認証子ＤＭＡＣと読み出した認証子ＭＡＣとが一致するか否かを判断する。一致すると判断する場合に、スイッチ１２１１へ、閉じる指示を出力し、一致しないと判断する場合に、スイッチ１２１１へ、開く指示を出力する。

（８）スイッチ１２１１

スイッチ１２１１は、比較部１２０６からの指示により、開閉が制御される。スイッチ１２１１は、比較部１２０６から閉じる指示を受け取った場合に、閉じ、開く指示を受け取った場合に、開く。

また、スイッチ１２１１は、鍵計算部１２０２から復号メディア鍵ｙを受け取る。閉じる指示を受け取った場合に、受け取った復号メディア鍵ｙを復号部

１２０４へ出力する。開く指示を受け取った場合に、復号メディア鍵ｙは、外部へ出力されない。

（９）復号部１２０４

復号部１２０４は、スイッチ１２１１から復号メディア鍵ｙを受け取る。また、指定受付部１２０７からコンテンツ番号を受け取り、ドライブ部１２１３を介して、記録媒体１３００上において、受け取った前記コンテンツ番号が付加された暗号化コンテンツファイル１３２０を特定し、特定された暗号化コンテンツファイル１３２０の鍵記録部１３２３に記録されている暗号化コンテンツ鍵ＥＣＫを読み出し、受け取った復号メディア鍵ｙを用いて、読み出した暗号化コンテンツ鍵ＥＣＫに復号アルゴリズムＤ２を施して復号コンテンツ鍵ＤＣＫを生成し、生成した復号コンテンツ鍵ＤＣＫを復号部１２０５へ出力する。

（１０）復号部１２０５

復号部１２０５は、復号部１２０４から復号コンテンツ鍵ＤＣＫを受け取る。また、指定受付部１２０７からコンテンツ番号を受け取り、ドライブ部１２１３を介して、記録媒体１３００上において、受け取った前記コンテンツ番号が付加された暗号化コンテンツファイル１３２０を特定し、特定された暗号化コンテンツファイル１３２０のコンテンツ記録部１３２４に記録されている暗号化コンテンツＥＣＮＴを読み出し、受け取った復号コンテンツ鍵ＤＣＫを用いて、読み出した暗号化コンテンツＥＣＮＴに復号アルゴリズムＤ３を施して復号コンテンツＤＣＮＴを生成し、生成した復号コンテンツＤＣＮＴを再生部１２１４へ出力する。

（１１）再生部１２１４

再生部１２１４は、復号部１２０５から復号コンテンツＤＣＮＴを受け取り、受け取った復号コンテンツＤＣＮＴから映像情報及び音声情報を生成し、生成した映像情報及び音声情報をアナログの映像信号及び音声信号に変換し、アナログの映像信号及び音声信号をモニタ１２９０へ出力する。

（１２）制御部１２１５、入力部１２１６、表示部１２１７、ドライブ部１２１３、モニタ１２９０及びリモコン１２８０

制御部１２１５は、再生装置１２００を構成する各構成要素の動作を制御する。

リモコン１２８０は、各種のボタンを備え、操作者の前記ボタンの操作に応じた操作指示情報を生成し、生成した操作指示情報を赤外線に乗せて出力する。

入力部１２１６は、リモコン１２８０から、操作指示情報が乗せられた赤外線を受け取り、受け取った赤外線から操作指示情報を抽出し、抽出した操作指示情報を制御部１２１５又は指定受付部１２０７へ出力する。

表示部１２１７は、制御部１２１５の制御の基に、様々な情報を表示する。

ドライブ部１２１３は、記録媒体１３００からの情報の読み出しを行う。

モニタ１２９０は、ＣＲＴ及びスピーカを備え、再生部１２１４からアナログの映像信号及び音声信号を受信し、映像信号に基づいて映像を表示し、音声信号に基づいて音声を出力する。

２．７　記録媒体に記録されるデータの構造と関連処理

（１）バージョン番号

図１２において、バージョン番号は、１６進数４桁で表現されており、具体的には、「３」である。第２の実施の形態では、配信局装置１４００から、鍵無効化データのバージョン番号が割当てられる。

具体的には、最初に発行された鍵無効化データには、バージョン番号として「１」が割当てられ、その後、発行される鍵無効化データには、バージョン番号が「２」、「３」、・・・というように割当てられる。

鍵無効化が発生した場合、新しい鍵無効化データが発行され、その際に新しいバージョン番号が付与される。なお、新しい鍵無効化データの発行は、鍵無効化が発生した場合のみに限定されない。例えば、セキュリティの観点から、予め定められた一定期間ごとに新しい鍵無効化データの発行を行うとしてもよい。

（２）鍵無効化データ識別子

図１２において、識別子記録部１３１２に記録されている鍵無効化データ識別子は、１６進数４桁で表現されており、鍵無効化データ識別子ＲＩＤは、「１」である。

ここで、鍵無効化データ識別子ＲＩＤは、記録媒体毎に、それぞれ記録される鍵無効化データを一意に識別するための情報である。従って、記録媒体毎に独立した体系により、鍵無効化データ識別子を割り当てることができる。

記録装置１１００の割当部１１０７による鍵無効化データ識別子ＲＩＤの具体的な割当て方法としては、割当部１１０７は、既に記録媒体に記録されている鍵無効化データに割当てられた鍵無効化データ識別子とは異なる値を割り当てる。

例えば、図１４に示すように、記録媒体１３００ａに、既に鍵無効化データファイル１と鍵無効化データファイル２とが記録されており、それぞれの鍵無効化データ識別子は、「１」及び「２」であるとする。

このとき、この記録媒体に新たな鍵無効化データファイル３を記録する際、割当部１１０７は、鍵無効化データ識別子ＲＩＤとして、「１」及び「２」以外の値、例えば「３」を割当てる。

（３）デバイス鍵とメディア鍵

図１２において、データ記録部１３１３には、ｎ個のデバイス鍵ＤＫ＿ｉ（ｉ＝１、２、・・・、ｎ）を用いて、メディア鍵ＭＫを、それぞれ暗号化することにより得られる暗号化メディア鍵Ｅ（ＤＫ＿ｉ、ＭＫ）が記録されている。

また、図１２において、装置ｎが保有するデバイス鍵をＤＫ＿ｎと表現している。この図の例では、装置３、並びに装置４が無効化されているため、それぞれが保有するＤＫ＿３、及びＤＫ＿４では、メディア鍵ＭＫとは全く無関係のデータ「０」が暗号化されて記録されている。

鍵無効化データをこのように生成することで、例えば、デバイス鍵ＤＫ＿１を保有する装置１は、鍵無効化データのＥ（ＤＫ＿１，ＭＫ）をデバイス鍵ＤＫ＿１で復号することにより、メディア鍵ＭＫを得ることができるが、デバイス鍵ＤＫ＿３を保有する装置３は、鍵無効化データのＥ（ＤＫ＿３，０）をデバイス鍵ＤＫ＿３で復号したとしても、メディア鍵ＭＫを得ることができない。

このように、図１２の例では、装置３及び装置４以外の全ての装置だけが正しいメディア鍵ＭＫを共有でき、装置３及び装置４は、正しいメディア鍵ＭＫが得らない。こうして、無効化された装置３及び装置４を、システムから排除することができる。

なお、装置の無効化方法は他の方法を利用してもよく、例えば、特許文献１には木構造を利用した無効化方法が開示されている。

（４）暗号化コンテンツファイル

図１２において、暗号化コンテンツファイル１３２０は、識別子記録部１３２１、認証子記録部１３２２、鍵記録部１３２３及びコンテンツ記録部１３２４からなる。

この図において、識別子記録部１３２１に記録されている鍵無効化データ識別子は、１６進数４桁で表現されており、鍵無効化データ識別子ＲＩＤは、具体的には、「１」である。

鍵無効化データ識別子ＲＩＤは、以下で説明するように、再生装置１２００において、再生したい暗号化コンテンツを復号するために使用する鍵無効化データファイル３１０を記録媒体１３００から取得するために使用される。

即ち、再生装置１２００において、記録媒体１３００に記録された暗号化コンテンツを復号再生する際、再生したい暗号化コンテンツファイル１３２０の識別子記録部１３２１に記録されている鍵無効化データ識別子ＲＩＤと同じ鍵無効化ＩＤを識別子記録部１３１２に含む鍵無効化データファイル３１０を、記録媒体１３００から取得する。

ここで、図１５を用いてより具体的に説明する。図１５に示すように、記録媒体１３００ｂには、鍵無効化データファイル１、鍵無効化データファイル２、暗号化コンテンツファイルＡ、暗号化コンテンツファイルＢ及び暗号化コンテンツファイルＣが記録されている。

この図に示すように、鍵無効化データファイル１及び鍵無効化データファイルの鍵無効化データ識別子は、それぞれ、「１」及び「２」である。また、暗号化コンテンツファイルＡ、暗号化コンテンツファイルＢ及び暗号化コンテンツファイルＣの鍵無効化データ識別子は、それぞれ、「１」、「１」及び「２」である。

これは、記録装置１１００において、暗号化コンテンツファイルＡを生成し記録する際、鍵無効化データファイル１の鍵無効化データを使用し、暗号化コンテンツファイルＢを生成し記録する際、鍵無効化データファイル１の鍵無効化データを使用し、暗号化コンテンツファイルＣを生成し記録する際、鍵無効化データファイル２の鍵無効化データを使用したことを表している。

このとき、再生装置１２００は、例えば、図１５に示す記録媒体１３００ｂにおける暗号化コンテンツファイルＢを復号して再生する場合には、暗号化コ

ンテンツファイルＢの鍵無効化データ識別子は「１」であるから、鍵無効化データ識別子が「１」である鍵無効化データファイル１を取得し、所得した鍵無効化データファイル１に含まれている鍵無効化データを使用して、暗号化コンテンツファイルＢに格納されている暗号化コンテンツを復号する。

２．８　コンテンツ供給システム２０の動作

コンテンツ供給システム２０の動作について、特に、記録装置１１００による記録媒体１３００へのデータの書き込みの動作及び再生装置１２００による記録媒体１３００に記録されているデータの再生の動作について、説明する。

（１）記録装置１１００による書き込みの動作

記録装置１１００による記録媒体１３００へのデータの書き込みの動作について、図１６～図１８に示すフローチャートを用いて説明する。

記録装置１１００の送受信部１１１１は、配信局装置１４００から、インターネット４０を介して、鍵無効化データＲＤＡＴＡ及びバージョン番号ＶＲを受信し、受信した鍵無効化データＲＤＡＴＡ及びバージョン番号ＶＲを、対応付けて、無効化データ格納部１１０２に格納する（ステップＳ１５０１）。

なお、ステップＳ１５０１における鍵無効化データＲＤＡＴＡ及びバージョン番号ＶＲの受信は、配信局装置１４００により、新しい鍵無効化データＲＤＡＴＡが発行された時に行われる。鍵無効化データＲＤＡＴＡには、上述したように、その発行順序を示すバージョン番号ＶＲが付加されている。記録装置１１００は、このバージョン番号ＶＲに基づいて、受信した鍵無効化データＲＤＡＴＡが新しいものかどうかを確認する。

例えば、記録装置１１００の無効化データ格納部１１０２が、バージョン番号「１」が付加された鍵無効化データを保持している場合、配信局装置１４００からバージョン番号「２」が付加された鍵無効化データを受信したと想定するとき、記録装置１１００の制御部１１０９は、受信した鍵無効化データに付加されたバージョン番号「２」と、無効化データ格納部１１０２に保持されている鍵無効化データに付加されたバージョン番号「１」とを比較する。受信した鍵無効化データに付加されたバージョン番号「２」の方が新しいので、制御部１１０９は、受信した鍵無効化データは、新しいものであるとして、受信した鍵無効化データとバージョン番号「２」とを無効化データ格納部１１０２に

格納するように送受信部１１１１へ指示を行う。ここで、バージョン番号は、その値が大きいほど、新しいことを示しているものとする。

なお、ここでは鍵無効化データの新旧の比較にバージョン番号を用いる場合について説明したが、この方法には限定されない。例えば、バージョン番号の代わりに、鍵無効化データには、その発行日時が付加されており、鍵無効化データの発行日時を用いて、鍵無効化データの新旧を比較する構成としてもよい。また、ここでは、配信局装置１４００から鍵無効化データを入手するとしたが、鍵無効化データの取得方法はこの構成に限定されない。例えば、鍵無効化データとバージョン番号とが記録された記録媒体が配布され、記録装置１１００は、この記録媒体から鍵無効化データとバージョン番号とを読み出すとしてもよい。

次に、記録装置１１００の比較部１１０８は、ドライブ部１１１０を介して、記録媒体１３００の記録領域１３０５に鍵無効化データファイルが存在するか否かを確認する。鍵無効化データファイルが存在しないと確認された場合は（ステップＳ１５０２）、後述するステップＳ１５０５ａに進む。

鍵無効化データファイル３１０が存在すると確認された場合は（ステップＳ１５０２）、比較部１１０８は、存在する全ての鍵無効化データファイルの版数記録部に記録されているバージョン番号について、ステップＳ１５０１で入手した鍵無効化データに付加されたバージョン番号と同じ内容のものが存在するか否かを確認する（ステップＳ１５０３）。

ステップＳ１５０３において、上記条件を満たすバージョン番号が存在しない場合は（ステップＳ１５０４）、後述するステップＳ１５０５ａに進む。

ステップＳ１５０４において、上記条件を満たすバージョン番号が存在する場合は（ステップＳ１５０４）、制御部１１０９は、ドライブ部１１１０を介して、上記条件を満たすバージョン番号を含む鍵無効化データファイル１３１０の識別子記録部１３１２より、鍵無効化データ識別子ＲＩＤを読み出す（ステップＳ１５０５）。

鍵計算部１１０３は、デバイス鍵格納部１０１からデバイス鍵を読み出し、無効化データ格納部１１０２から鍵無効化データを読み出し（ステップＳ１５０６）、読み出した鍵無効化データを読み出したデバイス鍵で復号することによりメディア鍵ＭＫを算出する（ステップＳ１５０７）。

次に、暗号化部１１０５は、算出されたメディア鍵を用いて、コンテンツサーバ装置１５００から受信したコンテンツ鍵ＣＫを暗号化して、暗号化コンテンツ鍵ＥＣＫを生成する（ステップＳ１５０８）。

認証子生成部１１０４は、記録媒体１３００の固有番号記録領域１３０１から媒体固有番号ＭＩＤを読み出し（ステップＳ１５０９）、鍵計算部１１０３により算出されたメディア鍵ＭＫと、暗号化部１１０５により生成された暗号化コンテンツ鍵ＥＣＫと、読み出した媒体固有番号ＭＩＤとを結合した値をハッシュ関数の入力値としたときの出力値として、認証子ＭＡＣを生成する（ステップＳ１５１０）。なお、ここで使用するハッシュ関数は、公知の技術で実現可能である。例えばハッシュ関数としてＳＨＡ－１を使用するとしてもよい。なお、ＳＨＡ－１には限定されない。

次に、暗号化部１１０６は、コンテンツサーバ装置１５００から受信したコンテンツ鍵ＣＫを用いて、同じく受信したコンテンツＣＮＴを暗号化する（ステップＳ１５１１）。

記録装置１１００は、ステップＳ１５０５で取得した、又はステップＳ１５０５ａで割当てられた鍵無効化データ識別子ＲＩＤと、ステップＳ１５１０で生成した認証子ＭＡＣと、ステップＳ１５０８で生成した暗号化コンテンツ鍵と、ステップＳ１５１１で生成した暗号化コンテンツとを含む暗号化コンテンツファイルを、記録媒体１３００の記録領域１３０５に記録し（ステップＳ１５１２）、処理を終了する。

また、記録媒体１３００に鍵無効化データファイル１３１０が存在しないと確認された場合（ステップＳ１５０２）、及びステップＳ１５０３において条件を満たすバージョン番号が存在しない場合は（ステップＳ１５０４）、割当部１１０７は、ステップＳ１５０１で入手した鍵無効化データに対して、記録媒体１３００の記録領域１３０５に記録されている全ての鍵無効化データファイルに既に割当てられた鍵無効化データ識別子ＲＩＤとは異なる値を、鍵無効化データ識別子として、割当てる（ステップＳ１５０５ａ）。

例えば、記録媒体１３００に、鍵無効化データファイルが一切存在しない場合には、割当部１１０７は、任意の値、例えば「１」を割当る。また、図１４に示す例のように、記録媒体１３００ａに、鍵無効化データ識別子ＲＩＤが「１」

及び「２」の鍵無効化データファイル１及び２が存在する場合には、割当部１１０７は、「１」及び「２」とは異なる値、例えば「３」を割当てる。

次に、記録装置１１００のドライブ部１１１０は、ステップＳ１５０１で入手した鍵無効化データと、その鍵無効化データのバージョン番号と、ステップＳ１５０５ａで割当てられた鍵無効化データ識別子とを有する鍵無効化データファイルを、記録媒体１３００の鍵無効化データファイル１３０２に記録する（ステップＳ１５０５ｂ）。このとき、鍵無効化データ、バージョン番号及び鍵無効化データ識別子ＲＩＤを、ぞれぞれ、鍵無効化データファイル３１０のデータ記録部１３１３、版数記録部１３１１及び識別子記録部１３１２に記録する。次に、ステップＳ１５０６へ制御が移り、以降、前述したステップＳ１５０６からステップＳ１５１２までが実行される。

（２）再生装置１２００による再生の動作

再生装置１２００による記録媒体１３００に記録されているデータの再生の動作について、図１９～図２０に示すフローチャートを用いて説明する。

再生装置１２００の指定受付部１２０７は、再生すべきコンテンツの指定を受け付ける（ステップＳ１６０１）。

取得部１２０８は、記録媒体１３００の記録領域１３０５より、ステップＳ１６０１で指定されたコンテンツに対応する暗号化コンテンツファイルを見出す（ステップＳ１６０２）。

なお、指定受付部１２０７における再生すべきコンテンツの指定方法、及び、指定されたコンテンツに対応する暗号化コンテンツファイルの見出し方法としては、例えば、再生装置１２００は、記録媒体１３００の記録領域１３０５に記録されている全ての暗号化コンテンツファイルの属性を示す情報（例えば、暗号化コンテンツのファイル名、コンテンツのタイトル名、コンテンツの記録日時、コンテンツの要約情報、コンテンツのサムネイル画像、コンテンツを示すアイコンなど）の一覧を、再生装置１２００の表示部１２１７に表示し、利用者に、その一覧の中から、再生したいコンテンツを選択させることにより、再生すべきコンテンツの指定を受け付ける。また、再生装置１２００は、指定されたコンテンツの属性情報から、指定されたコンテンツが格納された暗号化コンテンツファイルのファイル名を知り、記録媒体１３００の記録領域１３０

５から、該当のファイル名の暗号化コンテンツファイルを見出す。

なお、暗号化コンテンツファイルの見出し方法としては、上述の方法に限定されるものではなく、他の方法を用いてもよい。

取得部１２０８は、ステップＳ１６０２で見出した暗号化コンテンツファイル１３２０の識別子記録部１３２１より鍵無効化データ識別子を読み出す（ステップＳ１６０３）。

検索部１２０９は、記録媒体１３００の記録領域１３０５より、ステップＳ１６０３で読み出した鍵無効化データ識別子ＲＩＤと同じ値が、識別子記録部１３１２に記録されている鍵無効化データファイル３１０を見出す（ステップＳ１６０４）。次に、検索部１２０９は、ステップＳ１６０４で見出した鍵無効化データファイル１３１０を取得する（ステップＳ１６０５）。

鍵計算部１２０２は、デバイス鍵格納部１２０１からデバイス鍵を読出し、検索部１２０９から鍵無効化データを受け取る（ステップＳ１６０６）。

鍵計算部１２０２は、ステップＳ１６０６で受け取った鍵無効化データを、デバイス鍵を用いて復号することにより復号メディア鍵ｙを算出する（ステップＳ１６０７）。

認証子生成部１２０３は、記録媒体１３００の固有番号記録領域１３０１から媒体固有番号ＭＩＤを読み出し（ステップＳ１６０８）、ステップＳ１６０２で見出した暗号化コンテンツファイル１３２０の鍵記録部１３２３より暗号化コンテンツ鍵ＥＣＫを読み出し（ステップＳ１６０９）、ステップＳ１６０７で取得した復号メディア鍵ｙと、ステップＳ１６０９で読み出した暗号化コンテンツ鍵ＥＣＫと、ステップＳ１６０８で取得した媒体固有番号ＭＩＤとを結合した値をハッシュ関数の入力値としたときの出力値として、復号認証子ＤＭＡＣを生成する（ステップＳ１６１０）。ここで使用するハッシュ関数は、記録装置１１００で用いたものと同じハッシュ関数ＳＨＡ－１である。

比較部１２０６は、ステップＳ１６０２で見出した暗号化コンテンツファイル１３２０の認証子記録部３２２より、認証子ＭＡＣを読み出し（ステップＳ１６１１）、ステップＳ１６１０で算出された復号認証子ＤＭＡＣとステップＳ１６１１で読み出した認証子ＭＡＣが一致するかどうか確認する（ステップＳ１６１２）。

復号認証子ＤＭＡＣと認証子ＭＡＣとが一致しなければ（ステップＳ１６１３）、再生動作は、終了する。

復号認証子ＤＭＡＣと認証子ＭＡＣとが一致すれば(ステップＳ１６１３)、復号部１２０４は、暗号化コンテンツ鍵を、ステップＳ１６０７で算出した復号メディア鍵ｙで復号し、復号コンテンツ鍵ＤＣＫを取得する（ステップＳ１６１４）。

復号部１２０５は、ステップＳ１６０２で見出した暗号化コンテンツファイル１３２０のコンテンツ記録部１３２４より､暗号化コンテンツを読み出し(ステップＳ１６１５）、ステップＳ１６１５で読み出した暗号化コンテンツを、ステップＳ１６１４で復号した復号コンテンツ鍵ＤＣＫを用いて、復号して復号コンテンツし、再生部１２１４は、復号コンテンツを再生する（ステップＳ１６１６）。

２．９　その他の変形例

以下に示すように構成してもよい。

（１）第２の実施の形態においては、鍵無効化データの世代を示すバージョン番号及び鍵無効化データを識別する鍵無効化データ識別子を、それぞれ、鍵無効化データファイルにおける版数記録部及び識別子記録部に記録するとしたが、この方法に限定されない。

例えば、鍵無効化データファイルを識別するファイル名の一部に、鍵無効化データのバージョン番号と鍵無効化データ識別子の両者、又は少なくとも１つを含む構成としても良い。具体的には、鍵無効化データファイルのファイル名を、“ＫＲＤ＿ｎ＿ｍ”としてもよい。ここで、ｎはバージョン番号であり、ｍは鍵無効化データ識別子である。この場合、例えば、“ＫＲＤ＿０００１＿０００２”というファイル名により識別される鍵無効化データファイルのバージョン番号は「１」であり、鍵無効化データ識別子ＲＩＤは「２」である。

このようにファイル名にバージョン番号や鍵無効化データ識別子の両者、又は少なくとも１つ含めることにより、再生装置は、ファイル名を見れば、鍵無効化データファイルのバージョン番号や鍵無効化データ識別子ＲＩＤを知ることができ、再生装置におけるファイルを検索する際の処理が軽減できるというメリットがある。

（2）第2の実施の形態においては、鍵無効化データ識別子を、暗号化コンテンツファイルにおける識別子記録部に記録するとしたが、この方法に限定されない。

例えば、暗号化コンテンツファイルを識別するファイル名の一部に鍵無効化データ識別子を含める構成としても良い。具体的には、暗号化コンテンツを識別するファイル名を、“ＥＣＮＴ＿m”としてもよい。ここで、mは、鍵無効化データ識別子である。例えば“ＥＣＮＴ＿０００２”というファイル名の暗号化コンテンツファイルの鍵無効化データ識別子ＲＩＤは「２」である。

このようにファイル名に鍵無効化データ識別子を含めることにより、再生装置において、ファイル名を見れば、鍵無効化データ識別子を知ることができ、再生装置における鍵無効化データ識別子の取得する際の処理が軽減できるというメリットがある。

（3）第２の実施の形態においては、鍵無効化データを鍵無効化データ識別子と関連づけるため、また暗号化コンテンツを前記鍵無効化データ識別子ＲＩＤと関連づけるために、鍵無効化データファイル１３１０に、版数記録部１３１１と、識別子記録部１３１２を設け、それぞれ、バージョン番号と鍵無効化データ識別子とを記録し、暗号化コンテンツファイル１３２０に識別子記録部１３２１を設け、鍵無効化データ識別子を記録する構成としているが、この構成に限定されない。

例えば、記録装置は、記録媒体１３００上に、１個以上の鍵無効化データファイルと、１個以上の暗号化コンテンツファイルと、１個の鍵無効化データ管理ファイルとを記録するとしてもよい。この鍵無効化データ管理ファイルには、鍵無効化データファイル毎に、その鍵無効化データのバージョン番号と、鍵無効化データ識別子と、記録媒体上で該鍵無効化データファイルを一意に特定するための情報（例えば、鍵無効化データファイルが記録されているディレクトリ名やファイル名など）と、該鍵無効化データファイルを用いて暗号化した暗号化コンテンツファイルを記録媒体上で一意に特定するための情報（例えば、暗号化コンテンツファイルが記録されているディレクトリ名やファイル名など）とが含まれる。再生装置は、この鍵無効化データ管理ファイルに記録されている上記情報に基づいて、再生が指定された暗号化コンテンツに関連する鍵

無効化データファイルを取得する。

また、本実施の形態の構成と、鍵無効化データ管理ファイルを設ける構成を組み合わせた構成としても良い。

（４）第２の実施の形態では、鍵無効化データのバージョン番号と、鍵無効化データ識別子の両方が存在する構成としたが、この構成には限定されず、鍵無効化データ識別子だけが存在する構成でもよい。

（５）第２の実施の形態では、鍵無効化技術として、記録媒体の書き換え可能領域に記録する鍵無効化データを、無効化されていない装置が保有するデバイス鍵用いてメディア鍵を暗号化したものと、無効化された装置が保有するデバイス鍵を用いてメディア鍵とは無関係な値（例えば「０」）を暗号化したものとし、記録媒体の書き換え可能領域に記録する暗号化コンテンツを、コンテンツを前記メディア鍵に基づいて暗号化したものとする場合について説明したが、この構成に限定されるものではない。

例えば、記録媒体の書き換え可能領域に記録する鍵無効化データと暗号化コンテンツとして、無効化されていない装置においては、鍵無効化データに基づいて暗号化コンテンツが復号再生でき、無効化された装置においては、鍵無効化データに基づいて暗号化コンテンツが復号再生できないという条件を満たすものであればどんな構成であってもよい。

（６）第２の実施の形態では、メディアバインド技術として、記録装置１１００において媒体固有番号ＭＩＤを用いて認証子ＭＡＣを生成して、再生装置１２００において認証子ＭＡＣの比較を行うとしているが、この構成に限定されるものではない。

例えば、記録装置１１００において媒体固有番号ＭＩＤを用いてコンテンツを暗号化して記録媒体に記録し、再生装置１２００において媒体固有番号ＭＩＤを用いて暗号化されたコンテンツを復号する構成としても良い。

（７）第２の実施の形態では、鍵無効化データ識別子を割り当てる際、記録装置１１００に既に記録されている鍵無効化データに割当てられていない値を、鍵無効化ＩＤとして割当てる構成としているが、この構成に限定されるものではない。

例えば、記録装置１１００は、既に割当てた鍵無効化データ識別子を媒体固

有番号ＭＩＤとともに記憶しておき、記録装置１１００に記憶している上記情報に基づいて、鍵無効化データ識別子を割り当てる構成としても良い。

２．１０　まとめ

以上の説明から明らかなように、本発明に係る記録装置は、特定装置が保有する鍵を無効化するための鍵無効化データを格納する鍵無効化データ格納手段と、前記鍵無効化データに基づいて前記コンテンツを暗号化するコンテンツ暗号化手段と、前記鍵無効化データに対して、前記記録媒体において前記鍵無効化データを一意に識別するための鍵無効化データ識別情報を割当てる鍵無効化データ識別情報割当手段と、前記記録媒体に、前記鍵無効化データを前記鍵無効化データ識別情報と関連づけて記録する鍵無効化データ記録手段と、前記暗号化コンテンツを前記鍵無効化データ識別情報と関連づけて記録する暗号化コンテンツ記録手段とを備える。

また、本発明の記録装置における前記鍵無効化データ識別情報割当手段は、前記記録媒体に記録されている鍵無効化データに既に割当てられた鍵無効化データ識別情報とは異なる値を、鍵無効化データ識別情報情報として割当てる。

また、本発明の記録装置における前記鍵無効化データ識別情報割当手段は、前記記録媒体に記録されている鍵無効化データと、前記鍵無効化データ格納手段に格納されている鍵無効化データの新旧を比較し、前記鍵無効化データ格納手段に格納されている鍵無効化データが新しい場合のみ、鍵無効化データ識別情報の割当てを行うことを特徴とする。

また、本発明における記録装置における前記鍵無効化データ識別情報割当手段は、前記記録媒体に記録されている鍵無効化データと、前記鍵無効化データ格納手段に格納されている鍵無効化データの新旧の比較を、各鍵無効化データが生成された日時に関連する情報、もしくは、各鍵無効化データが生成された順序に関連する情報に基づいて行う。

また、本発明に係る再生装置は、前記記録媒体から、暗号化コンテンツと、前記暗号化コンテンツに関連づけて記録された鍵無効化データ識別情報を読み出す暗号化コンテンツ読出手段と、前記記録媒体から、前記暗号化コンテンツ読出手段にて読み出した鍵無効化データ識別情報と同じ鍵無効化データ識別情報が関連づけて記録されている鍵無効化データを読み出す鍵無効化データ読出

手段と、前記鍵無効化データ読出手段にて読み出した鍵無効化データに基づいて前記暗号化コンテンツ読出手段で読み出した前記暗号化コンテンツを復号するコンテンツ復号手段とを備える。

また、本発明における記録媒体は、鍵無効化データを、前記記録媒体においてこの鍵無効化データを一意に識別するための鍵無効化データ識別情報と関連づけて記録する鍵無効化データ格納手段と、前記鍵無効化データに基づいて暗号化された暗号化コンテンツを前記無効化データ識別情報と関連づけて記録する暗号化コンテンツ格納手段とを備える。

また、本発明における前記記録媒体は、さらに、鍵無効化データの新旧を示す情報を、鍵無効化データと関連づけて記録する。

また、本発明における著作権保護システムは、記録装置と、記録媒体と、再生装置からなり、前記記録装置は、特定装置が保有する鍵を無効化するための鍵無効化データを格納する鍵無効化データ格納手段と、前記鍵無効化データに基づいて前記コンテンツを暗号化するコンテンツ暗号化手段と、前記鍵無効化データに対して、前記記録媒体において前記鍵無効化データを一意に識別するための鍵無効化データ識別情報を割当てる鍵無効化データ識別情報割当手段と、前記記録媒体に、前記鍵無効化データを前記鍵無効化データ識別情報と関連づけて記録する鍵無効化データ記録手段と、前記暗号化コンテンツを前記鍵無効化データ識別情報と関連づけて記録する暗号化コンテンツ記録手段とを備え、前記記録媒体は、前記鍵無効化データを前記鍵無効化データ識別情報と関連づけて記録する鍵無効化データ格納手段と、前記暗号化コンテンツを前記無効化データ識別情報と関連づけて記録する暗号化コンテンツ格納手段とを備え、前記再生装置は、前記記録媒体から、暗号化コンテンツと、前記暗号化コンテンツに関連づけて記録された鍵無効化データ識別情報を読み出す暗号化コンテンツ読出手段と、前記暗号化コンテンツ読出手段にて読み出した鍵無効化データ識別情報と同じ鍵無効化データ識別情報が関連づけて記録されている鍵無効化データを読み出す鍵無効化データ読出手段と、前記鍵無効化データ読出手段にて読み出した鍵無効化データに基づいて前記暗号化コンテンツ読出手段で読み出した前記暗号化コンテンツを復号するコンテンツ復号手段とを備える。

このように、第２の実施の形態に係る記録装置、記録媒体、再生装置、及び、

著作権保護システムにおいては、記録媒体に記録する鍵無効化データに対して、記録媒体においてその鍵無効化データを一意に識別するための鍵無効化データＩＤを割当て、この鍵無効化データＩＤを、記録媒体に記録する鍵無効化データと関連づけて鍵無効化データファイルとして記録するとともに、この鍵無効化データＩＤを、該鍵無効化データを使用して暗号化したコンテンツと関連づけて、暗号化コンテンツファイルとして、記録することにより、再生装置において、該暗号化コンテンツを復号再生する場合に、記録媒体に、複数の暗号化コンテンツファイルと、複数の鍵無効化データファイルが記録されている場合においても、該暗号化コンテンツファイルに含まれる鍵無効化データＩＤと同じ鍵無効化データＩＤを含む鍵無効化データファイルを検索取得することができ、暗号化コンテンツファイルを取得した鍵無効化データファイルを用いて復号再生することが可能となる。

３．その他の変形例

なお、本発明を上記の各実施の形態に基づいて説明してきたが、本発明は、上記の実施の形態に限定されないのはもちろんである。以下のような場合も本発明に含まれる。

（１）各実施の形態において、コンテンツは、映像データと音声データとが高効率で圧縮符号化されたデータであるとしているが、これには、限定されない。　例えば、コンテンツは、小説、静止画像、音声などがデジタル化されたコンピュータデータであるとしてもよい。

また、例えば、コンテンツは、コンピュータを構成するマイクロプロセッサの動作を制御する複数の命令から構成されるコンピュータプログラムであるとしてもよい。また、表計算ソフトにより生成される表データであるとしてもよいし、データベースソフトにより生成されるデータベースであるとしてもよい。

（２）上記の各装置は、具体的には、マイクロプロセッサ、ＲＯＭ、ＲＡＭ、ハードディスクユニット、ディスプレィユニット、キーボード、マウスなどから構成されるコンピュータシステムである。前記ＲＡＭ又は前記ハードディスクユニットには、コンピュータプログラムが記憶されている。前記マイクロプロセッサが、前記コンピュータプログラムに従って動作することにより、各装置は、その機能を達成する。

（3）本発明は、上記に示す方法であるとしてもよい。また、これらの方法をコンピュータにより実現するコンピュータプログラムであるとしてもよいし、前記コンピュータプログラムからなるデジタル信号であるとしてもよい。

また、本発明は、前記コンピュータプログラム又は前記デジタル信号をコンピュータ読み取り可能な記録媒体、例えば、フレキシブルディスク、ハードディスク、ＣＤ—ＲＯＭ、ＭＯ、ＤＶＤ、ＤＶＤ－ＲＯＭ、ＤＶＤ－ＲＡＭ、ＢＤ（Ｂｌｕ－ｒａｙ　Ｄｉｓｃ）、半導体メモリなど、に記録したものとしてもよい。また、これらの記録媒体に記録されている前記コンピュータプログラム又は前記デジタル信号であるとしてもよい。

また、本発明は、前記コンピュータプログラム又は前記デジタル信号を、電気通信回線、無線又は有線通信回線、インターネットを代表とするネットワーク、データ放送等を経由して伝送するものとしてもよい。

また、本発明は、マイクロプロセッサとメモリとを備えたコンピュータシステムであって、前記メモリは、上記コンピュータプログラムを記憶しており、前記マイクロプロセッサは、前記コンピュータプログラムに従って動作するとしてもよい。

また、前記プログラム又は前記デジタル信号を前記記録媒体に記録して移送することにより、又は前記プログラム又は前記デジタル信号を前記ネットワーク等を経由して移送することにより、独立した他のコンピュータシステムにより実施するとしてもよい。

（4）上記各実施の形態及び上記各変形例をそれぞれ組み合わせるとしてもよい。

産業上の利用の可能性

本発明を構成する各装置及び記録媒体は、コンテンツを制作し、配給するコンテンツ配給産業において、経営的に、また継続的及び反復的に使用することができる。また、本発明を構成する各装置及び記録媒体は、電器機器製造産業において、経営的に、また継続的及び反復的に、製造し、販売することができる。

請　求　の　範　囲

1．記録媒体にコンテンツを暗号化して書き込む記録装置と、前記記録媒体に記録されている暗号化コンテンツの復号を試みる複数の再生装置とから構成される著作物保護システムであって、

前記複数の再生装置のうちいずれか1台以上は、無効化されており、

前記記録媒体は、読出専用の書換不可領域と、読出し及び書込みの可能な書換可能領域とを備え、前記書換不可領域には、当該記録媒体に固有の媒体固有番号が予め記録されており、

前記記録装置は、

無効化されていない各再生装置についてメディア鍵が、無効化された各再生装置について所定の検知情報が、それぞれ、当該再生装置のデバイス鍵を用いて、暗号化されて生成された複数の暗号化メディア鍵から構成されるメディア鍵データを記憶している記憶手段と、

前記記録媒体の前記書換不可領域から前記媒体固有番号を読み出す読出手段と、

読み出した前記媒体固有番号及び前記メディア鍵に基づいて、暗号化鍵を生成する生成手段と、

生成された前記暗号化鍵に基づいて、デジタルデータであるコンテンツを暗号化して暗号化コンテンツを生成する暗号化手段と、

前記記憶手段から前記メディア鍵データを読み出す読出手段と、

読み出された前記メディア鍵データ及び生成された前記暗号化コンテンツを前記記録媒体の前記書換可能領域に書き込む書込手段とを備え、

各再生装置は、

前記記録媒体の前記書換可能領域に書き込まれたメディア鍵データから当該再生装置に対応する暗号化メディア鍵を読み出す読出手段と、

当該再生装置のデバイス鍵を用いて、読み出された前記暗号化メディア鍵を復号して復号メディア鍵を生成する復号手段と、

生成された復号メディア鍵が、前記検知情報であるか否かを判断し、前記検

知情報である場合に、前記記録媒体に記録されている暗号化コンテンツの復号を禁止し、前記検知情報でない場合に、暗号化コンテンツの復号を許可する制御手段と、

復号が許可された場合に、前記記録媒体から前記暗号化コンテンツを読み出し、生成された復号メディア鍵に基づいて、読み出した前記暗号化コンテンツを復号して復号コンテンツを生成する復号手段と

を備えることを特徴とする著作物保護システム。

2．記録媒体にコンテンツを暗号化して書き込む記録装置と、前記記録媒体に記録されている暗号化コンテンツの復号を試みる複数の再生装置とから構成される著作物保護システムにおける前記記録装置であって、

前記複数の再生装置のうちいずれか1台以上は、無効化されており、

前記記録媒体は、読出専用の書換不可領域と、読出し及び書込みの可能な書換可能領域とを備え、前記書換不可領域には、当該記録媒体に固有の媒体固有番号が予め記録されており、

前記記録装置は、

無効化されていない各再生装置についてメディア鍵が、無効化された各再生装置について所定の検知情報が、それぞれ、当該再生装置のデバイス鍵を用いて、暗号化されて生成された複数の暗号化メディア鍵から構成されるメディア鍵データを記憶している記憶手段と、

前記記録媒体の前記書換不可領域から前記媒体固有番号を読み出す読出手段と、

読み出した前記媒体固有番号及び前記メディア鍵に基づいて、暗号化鍵を生成する生成手段と、

生成された前記暗号化鍵に基づいて、デジタルデータであるコンテンツを暗号化して暗号化コンテンツを生成する暗号化手段と、

前記記憶手段から前記メディア鍵データを読み出す読出手段と、

読み出された前記メディア鍵データ及び生成された前記暗号化コンテンツを前記記録媒体の前記書換可能領域に書き込む書込手段と

を備えることを特徴とする記録装置。

3．別の記録媒体は、無効化されていない各再生装置についてメディア鍵が、

無効化された各再生装置について所定の検知情報が、それぞれ、当該再生装置のデバイス鍵を用いて、暗号化されて生成された複数の別の暗号化メディア鍵から構成される別のメディア鍵データを記憶しており、

前記記録装置は、さらに、

前記別の記録媒体に記憶されている別のメディア鍵データと、前記記憶手段に記憶されている前記メディア鍵データとの新旧を比較する比較手段と、

前記別のメディア鍵データの方が新しいと判断される場合に、前記別の記録媒体から前記別のメディア鍵データを読み出し、読み出した前記別のメディア鍵データを、前記記憶手段に記憶されている前記メディア鍵データに、上書きする更新手段とを備え、

前記読出手段は、前記メディア鍵データの読出しに代えて、前記記憶手段から前記別のメディア鍵データを読み出し、

前記書込手段は、前記メディア鍵データの書込みに代えて、読み出された前記別のメディア鍵データを前記記録媒体の前記書換可能領域に書き込む

ことを特徴とする請求の範囲２に記載の記録装置。

４．前記記憶手段に記憶されている前記メディア鍵データは、当該メディア鍵データの世代を示す第１バージョン情報を含み、

前記別の記録媒体に記憶されている前記別のメディア鍵データは、当該別のメディア鍵データの世代を示す第２バージョン情報を含み、

前記比較手段は、前記第１バージョン情報と前記第２バージョン情報とを比較することにより、前記別のメディア鍵データと前記メディア鍵データとの新旧を比較する

ことを特徴とする請求の範囲３に記載の記録装置。

５．前記記憶手段に記憶されている前記メディア鍵データは、当該メディア鍵データが生成された日時を示す第１日時情報を含み、

前記別の記録媒体に記憶されている前記別のメディア鍵データは、当該別のメディア鍵データが生成された日時を示す第２日時情報を含み、

前記比較手段は、前記第１日時情報と前記第２日時情報とを比較することにより、前記別のメディア鍵データと前記メディア鍵データとの新旧を比較する

ことを特徴とする請求の範囲３に記載の記録装置。

6．前記記憶手段は、さらに、当該記録装置及び前記複数の再生装置のいずれかに割り当てられた公開鍵が無効化されていることを示す無効化データを記憶しており、

前記記録装置は、さらに、前記無効化データに対してデジタル署名を施して検証情報を生成する署名生成手段を備え、

前記書込手段は、さらに、生成した前記検証情報を前記記録媒体の前記書換可能領域に書き込む

ことを特徴とする請求の範囲２に記載の記録装置。

7．前記署名生成手段は、前記無効化データに対して、付録型の前記デジタル署名を施して署名データを生成し、生成した前記署名データと前記無効化データとから構成される前記検証情報を生成し、

前記書込手段は、前記署名データと前記無効化データとから構成される前記検証情報を書き込む

ことを特徴とする請求の範囲６に記載の記録装置。

8．前記署名生成手段は、前記無効化データに対して、回復型の前記デジタル署名を施して前記検証情報を生成する

ことを特徴とする請求の範囲６に記載の記録装置。

9．前記記憶手段は、さらに、当該記録装置の秘密鍵と公開鍵証明書とを記憶しており、

前記署名生成手段は、前記記憶手段に記憶されている前記秘密鍵を用いて、前記デジタル署名を施し、

前記読出手段は、さらに、前記記憶手段から前記公開鍵証明書を読み出し、

前記書込手段は、読み出された前記公開鍵証明書を前記記録媒体の前記書換可能領域に書き込む

ことを特徴とする請求の範囲６に記載の記録装置。

１０．前記記憶手段は、さらに、当該記録装置の公開鍵証明書を記憶しており、

前記読出手段は、さらに、前記記憶手段から前記公開鍵証明書を読み出し、

前記書込手段は、読み出された前記公開鍵証明書を前記記録媒体の前記書換可能領域に書き込む

ことを特徴とする請求の範囲２に記載の記録装置。

１１．前記記憶手段は、さらに、当該記録装置及び前記複数の再生装置のいずれかに割り当てられた公開鍵が無効化されていることを示す無効化データを記憶しており、

前記記録装置は、さらに、前記無効化データに対してデジタル署名を施して検証情報を生成する署名生成手段を備え、

前記書込手段は、さらに、生成した前記検証情報を別の記録媒体に書き込むことを特徴とする請求の範囲２に記載の記録装置。

１２．前記記憶手段は、さらに、当該記録装置及び前記複数の再生装置のいずれかに割り当てられた公開鍵が無効化されていることを示す無効化データを記憶しており、

前記読出手段は、さらに、前記記憶手段から前記無効化データを読み出し、

前記書込手段は、読み出された前記無効化データを別の記録媒体に書き込むことを特徴とする請求の範囲２に記載の記録装置。

１３．前記記憶手段は、さらに、当該記録装置の公開鍵証明書を記憶しており、

前記読出手段は、さらに、前記記憶手段から前記公開鍵証明書を読み出し、

前記書込手段は、読み出された前記公開鍵証明書を別の記録媒体に書き込むことを特徴とする請求の範囲２に記載の記録装置。

１４．前記記憶手段は、さらに、当該記録装置を識別する装置識別子を記憶しており、

前記記録装置は、さらに、

前記記憶手段から前記装置識別子を読み出し、読み出した前記装置識別子を前記コンテンツに電子透かしとして埋め込む埋込手段を備え、

前記暗号化手段は、前記装置識別子が埋め込まれたコンテンツを暗号化することを特徴とする請求の範囲２に記載の記録装置。

１５．前記記憶手段に記憶されている前記メディア鍵データは、さらに、当該メディア鍵データを識別するデータ識別子を含み、

前記書込手段は、前記データ識別子と前記暗号化コンテンツとを対応付けて、前記記録媒体の前記書換可能領域に書き込み、前記データ識別子を含む前記メディア鍵データを前記書換可能領域に書き込む

ことを特徴とする請求の範囲２に記載の記録装置。

１６．前記記録媒体は、さらに、無効化されていない各再生装置についてメディア鍵が、無効化された各再生装置について所定の検知情報が、それぞれ、当該再生装置のデバイス鍵を用いて、暗号化されて生成された複数の別の暗号化メディア鍵から構成される別のメディア鍵データを記憶しており、前記別のメディア鍵データは、当該メディア鍵データを識別する別のデータ識別子を含み、

前記記録装置は、さらに、

前記記録媒体に記録されている別のメディア鍵データを識別する前記別のデータ識別子とは、異なる前記データ識別子を前記記憶手段に記憶されている前記メディア鍵データに割り当てる割当手段を含む

ことを特徴とする請求の範囲１５に記載の記録装置。

１７．前記記録媒体は、さらに、

前記記憶手段に記憶されている前記メディア鍵データと、前記記録媒体に記録されている前記別のメディア鍵データとの新旧を比較する比較手段を含み、

前記割当手段は、前記記憶手段に記憶されている前記メディア鍵データの方が新しいと判断される場合に、前記データ識別子を割り当てる

ことを特徴とする請求の範囲１５に記載の記録装置。

１８．前記記憶手段に記憶されている前記メディア鍵データは、当該メディア鍵データが生成された日時を示す第１日時情報を含み、

前記記録媒体に記憶されている前記別のメディア鍵データは、当該別のメディア鍵データが生成された日時を示す第２日時情報を含み、

前記比較手段は、前記第１日時情報と前記第２日時情報とを比較することにより、前記別のメディア鍵データと前記メディア鍵データとの新旧を比較する

ことを特徴とする請求の範囲１７に記載の記録装置。

１９．記録媒体にコンテンツを暗号化して書き込む記録装置と、前記記録媒体に記録されている暗号化コンテンツの復号を試みる複数の再生装置とから構成される著作物保護システムにおける前記再生装置であって、

前記複数の再生装置のうちいずれか１台以上は、無効化されており、

前記記録媒体は、読出専用の書換不可領域と、読出し及び書込みの可能な書換可能領域とを備え、前記書換不可領域には、当該記録媒体に固有の媒体固有番号が予め記録されており、

前記記録装置は、無効化されていない各再生装置についてメディア鍵が、無効化された各再生装置について所定の検知情報が、それぞれ、当該再生装置のデバイス鍵を用いて、暗号化されて生成された複数の暗号化メディア鍵から構成されけるメディア鍵データを記憶しており、前記記録媒体の前記書換不可領域から前記媒体固有番号を読み出し、読み出した前記媒体固有番号及び前記メディア鍵に基づいて、暗号化鍵を生成し、生成された前記暗号化鍵に基づいて、デジタルデータであるコンテンツを暗号化して暗号化コンテンツを生成し、前記記憶手段から前記メディア鍵データを読み出し、読み出された前記メディア鍵データ及び生成された前記暗号化コンテンツを前記記録媒体の前記書換可能領域に書き込み、

前記再生装置は、

前記記録媒体の前記書換可能領域に書き込まれたメディア鍵データから当該再生装置に対応する暗号化メディア鍵を読み出す読出手段と、

当該再生装置のデバイス鍵を用いて、読み出された前記暗号化メディア鍵を復号して復号メディア鍵を生成する復号手段と、

生成された復号メディア鍵が、前記検知情報であるか否かを判断し、前記検知情報である場合に、前記記録媒体に記録されている暗号化コンテンツの復号を禁止し、前記検知情報でない場合に、暗号化コンテンツの復号を許可する制御手段と、

復号が許可された場合に、前記記録媒体から前記暗号化コンテンツを読み出し、生成された復号メディア鍵に基づいて、読み出した前記暗号化コンテンツを復号して復号コンテンツを生成する復号手段と

を備えることを特徴とする再生装置。

２０．前記記録装置は、さらに、当該記録装置及び前記複数の再生装置のいずれかに割り当てられた公開鍵が無効化されていることを示す無効化データを記憶しており、前記無効化データに対してデジタル署名を施して検証情報を生成し、生成した前記検証情報を前記記録媒体の前記書換可能領域に書き込み、

前記読出手段は、さらに、前記記録媒体の前記書換可能領域に書き込まれた前記検証情報を読み出し、

前記再生装置は、さらに、

読み出した前記検証情報に基づいて、署名検証を施して、検証の成功又は失敗を示す検証結果を出力する検証手段を備え、

前記制御手段は、さらに、前記検証結果が検証の失敗を示す場合に、前記暗号化コンテンツの復号を禁止し、前記検証結果が検証の成功を示す場合に、前記暗号化コンテンツの復号を許可する

ことを特徴とする請求の範囲１９に記載の再生装置。

２１．前記記録装置は、前記無効化データに対して、付録型の前記デジタル署名を施して署名データを生成し、生成した前記署名データと前記無効化データとから構成される前記検証情報を生成し、前記署名データと前記無効化データとから構成される前記検証情報を書き込み、

前記検証手段は、前記検証情報に含まれている前記署名データに基づいて、前記署名検証を施す

ことを特徴とする請求の範囲２０に記載の再生装置。

２２．前記記録装置は、前記無効化データに対して、回復型の前記デジタル署名を施して前記検証情報を生成し、

前記検証手段は、検証結果が成功の場合に、前記検証情報から前記無効化データを生成する

ことを特徴とする請求の範囲２０に記載の再生装置。

２３．前記記録装置は、さらに、当該記録装置の秘密鍵と公開鍵証明書とを記憶しており、記憶している前記秘密鍵を用いて、前記デジタル署名を施し、前記公開鍵証明書を読み出し、読み出した前記公開鍵証明書を前記記録媒体の前記書換可能領域に書き込み、

前記検証手段は、前記記録媒体から前記公開鍵証明書を読み出し、読み出した公開鍵証明書から公開鍵を抽出し、抽出した前記公開鍵を用いて、前記署名検証を施す

ことを特徴とする請求の範囲２０に記載の再生装置。

２４．前記記録装置は、さらに、当該記録装置及び前記複数の再生装置のいずれかに割り当てられた公開鍵が無効化されていることを示す無効化データを記憶しており、前記無効化データに対してデジタル署名を施して検証情報を生成し、生成した前記検証情報を別の記録媒体に書き込み、

前記読出手段は、前記記録媒体からの前記検証情報の読み出しに代えて、前記別の記録媒体から前記検証情報を読み出し、

前記検証手段は、前記別の記録媒体から読み出した前記検証情報に基づいて、署名検証を施す

ことを特徴とする請求の範囲２０に記載の再生装置。

２５．前記記録装置は、さらに、当該記録装置の公開鍵証明書を記憶しており、前記公開鍵証明書を読み出し、読み出した前記公開鍵証明書を前記記録媒体の前記書換可能領域に書き込み、

前記再生装置は、さらに、

前記記録装置及び前記複数の再生装置のいずれかに割り当てられた公開鍵が無効化されていることを示す第１無効化データを記憶している記憶手段と、

前記記録媒体から前記公開鍵証明書を読み出す証明書読出手段と、

読み出した公開鍵証明書に含まれる公開鍵が、前記第１無効化データにより、無効化されていることを示しているか否かを検証する公開鍵検証手段とを含み、

前記制御手段は、さらに、前記公開鍵が無効化されている場合に、前記暗号化コンテンツの復号を禁止し、前記公開鍵が無効化されていない場合に、前記暗号化コンテンツの復号を許可する

ことを特徴とする請求の範囲１９に記載の再生装置。

２６．別の記録媒体は、前記記録装置及び前記複数の再生装置のいずれかに割り当てられた公開鍵が無効化されていることを示す第２無効化データを記憶しており、

前記再生装置は、さらに、

前記別の記録媒体に記憶されている前記第２無効化データと、前記記憶手段に記憶されている前記第１無効化データとの新旧を比較する比較手段と、

前記第２無効化データの方が新しいと判断される場合に、前記別の記録媒体から前記第２無効化データを読み出し、読み出した前記第２無効化データを、前記記憶手段に記憶されている前記第１無効化データに、上書きする更新手段とを含む

ことを特徴とする請求の範囲２５に記載の再生装置。

２７．前記比較手段は、前記第１無効化データのサイズと前記第２無効化デー

タのサイズとを比較することにより、前記第１無効化データと前記第２無効化データとの新旧を比較する

ことを特徴とする請求の範囲２６に記載の再生装置。

２８．前記比較手段は、前記第１無効化データにより示される無効化された公開鍵の数と前記第２無効化データにより示される無効化された公開鍵の数とを比較することにより、前記第１無効化データと前記第２無効化データとの新旧を比較する

ことを特徴とする請求の範囲２６に記載の再生装置。

２９．前記記憶手段に記憶されている前記第２無効化データは、当該第２無効化データの世代を示す第２バージョン情報を含み、

前記別の記録媒体に記憶されている前記第１無効化データは、当該第１無効化データの世代を示す第１バージョン情報を含み、

前記比較手段は、前記第１バージョン情報と前記第２バージョン情報とを比較することにより、前記第１無効化データと第２無効化データとの新旧を比較する

ことを特徴とする請求の範囲２６に記載の再生装置。

３０．前記記憶手段に記憶されている前記第２無効化データは、当該第２無効化データが生成された日時を示す第２日時情報を含み、

前記別の記録媒体に記憶されている前記第１無効化データは、当該第１無効化データが生成された日時を示す第１日時情報を含み、

前記比較手段は、前記第１日時情報と前記第２日時情報とを比較することにより、前記第１無効化データと第２無効化データとの新旧を比較する

ことを特徴とする請求の範囲２６に記載の再生装置。

３１．前記記録装置は、さらに、当該記録装置及び前記複数の再生装置のいずれかに割り当てられた公開鍵が無効化されていることを示す第２無効化データを記憶しており、前記第２無効化データを読み出し、読み出した前記第２無効化データを別の記録媒体に書き込み、

前記公開鍵検証手段は、前記第１無効化データに代えて、前記別の記録媒体から前記第２無効化データを読み出し、読み出した前記第２無効化データにより、前記公開鍵が無効化されていることを示しているか否かを検証する

ことを特徴とする請求の範囲２５に記載の再生装置。

３２．前記記録装置は、さらに、当該記録装置の公開鍵証明書を記憶しており、前記公開鍵証明書を読み出し、読み出した前記公開鍵証明書を別の記録媒体に書き込み、

前記証明書読出手段は、前記記録媒体に代えて、前記別の記録媒体から前記公開鍵証明書を読み出す

ことを特徴とする請求の範囲２５に記載の再生装置。

３３．前記再生装置は、さらに、

当該再生装置を識別する装置識別子を記憶している前記記憶手段と、

復号が許可された場合に、前記記憶手段から前記装置識別子を読み出し、読み出した前記装置識別子を前記暗号化コンテンツに電子透かしとして埋め込む埋込手段と、

前記装置識別子が埋め込まれた前記暗号化コンテンツを前記記録媒体に書き込む

ことを特徴とする請求の範囲１９に記載の再生装置。

３４．前記記録装置に記憶されている前記メディア鍵データは、さらに、当該メディア鍵データを識別するデータ識別子を含み、前記記録装置は、前記データ識別子と前記暗号化コンテンツとを対応付けて、前記記録媒体の前記書換可能領域に書き込み、前記データ識別子を含む前記メディア鍵データを前記書換可能領域に書き込み、

前記再生装置は、さらに、

前記記録媒体に記録されている前記暗号化コンテンツの指定を受け付ける受付手段と、

指定が受け付けられた前記暗号化コンテンツに対応付けられた前記データ識別子を前記記録媒体から読み出す読出手段と、

読み出した前記データ識別子を含む前記メディア鍵データを前記記録媒体から読み出す読出手段とを含み、

前記制御手段は、読み出した前記メディア鍵データに基づいて、前記暗号化コンテンツの復号の可否を判断する

ことを特徴とする請求の範囲１９に記載の再生装置。

３５．記録媒体にコンテンツを暗号化して書き込む記録装置と、前記記録媒体に記録されている暗号化コンテンツの復号を試みる複数の再生装置とから構成される著作物保護システムにおける前記記録装置で用いられる記録方法であって、

前記複数の再生装置のうちいずれか１台以上は、無効化されており、

前記記録媒体は、読出専用の書換不可領域と、読出し及び書込みの可能な書換可能領域とを備え、前記書換不可領域には、当該記録媒体に固有の媒体固有番号が予め記録されており、

前記記録装置は、無効化されていない各再生装置についてメディア鍵が、無効化された各再生装置について所定の検知情報が、それぞれ、当該再生装置のデバイス鍵を用いて、暗号化されて生成された複数の暗号化メディア鍵から構成されるメディア鍵データを記憶している記憶手段を備え、

前記記録方法は、

前記記録媒体の前記書換不可領域から前記媒体固有番号を読み出す読出ステップと、

読み出した前記媒体固有番号及び前記メディア鍵に基づいて、暗号化鍵を生成する生成ステップと、

生成された前記暗号化鍵に基づいて、デジタルデータであるコンテンツを暗号化して暗号化コンテンツを生成する暗号化ステップと、

前記記憶手段から前記メディア鍵データを読み出す読出ステップと、

読み出された前記メディア鍵データ及び生成された前記暗号化コンテンツを前記記録媒体の前記書換可能領域に書き込む書込ステップと

を含むことを特徴とする記録方法。

３６．記録媒体にコンテンツを暗号化して書き込む記録装置と、前記記録媒体に記録されている暗号化コンテンツの復号を試みる複数の再生装置とから構成される著作物保護システムにおける前記記録装置で用いられる記録用のコンピュータプログラムであって、

前記複数の再生装置のうちいずれか１台以上は、無効化されており、

前記記録媒体は、読出専用の書換不可領域と、読出し及び書込みの可能な書換可能領域とを備え、前記書換不可領域には、当該記録媒体に固有の媒体固有

番号が予め記録されており、

前記記録装置は、無効化されていない各再生装置についてメディア鍵が、無効化された各再生装置について所定の検知情報が、それぞれ、当該再生装置のデバイス鍵を用いて、暗号化されて生成された複数の暗号化メディア鍵から構成されるメディア鍵データを記憶している記憶手段を備え、

前記記録用のコンピュータプログラムは、

前記記録媒体の前記書換不可領域から前記媒体固有番号を読み出す読出ステップと、

読み出した前記媒体固有番号及び前記メディア鍵に基づいて、暗号化鍵を生成する生成ステップと、

生成された前記暗号化鍵に基づいて、デジタルデータであるコンテンツを暗号化して暗号化コンテンツを生成する暗号化ステップと、

前記記憶手段から前記メディア鍵データを読み出す読出ステップと、

読み出された前記メディア鍵データ及び生成された前記暗号化コンテンツを前記記録媒体の前記書換可能領域に書き込む書込ステップと

を含むことを特徴とするコンピュータプログラム。

３７．前記コンピュータプログラムは、コンピュータ読み取り可能な記録媒体に記録されている

ことを特徴とする請求の範囲３７に記載のコンピュータプログラム。

３８．記録媒体にコンテンツを暗号化して書き込む記録装置と、前記記録媒体に記録されている暗号化コンテンツの復号を試みる複数の再生装置とから構成される著作物保護システムにおける前記再生装置で用いられる再生方法であって、

前記複数の再生装置のうちいずれか１台以上は、無効化されており、

前記記録媒体は、読出専用の書換不可領域と、読出し及び書込みの可能な書換可能領域とを備え、前記書換不可領域には、当該記録媒体に固有の媒体固有番号が予め記録されており、

前記記録装置は、無効化されていない各再生装置についてメディア鍵が、無効化された各再生装置について所定の検知情報が、それぞれ、当該再生装置のデバイス鍵を用いて、暗号化されて生成された複数の暗号化メディア鍵から構

成されけるメディア鍵データを記憶しており、前記記録媒体の前記書換不可領域から前記媒体固有番号を読み出し、読み出した前記媒体固有番号及び前記メディア鍵に基づいて、暗号化鍵を生成し、生成された前記暗号化鍵に基づいて、デジタルデータであるコンテンツを暗号化して暗号化コンテンツを生成し、前記記憶手段から前記メディア鍵データを読み出し、読み出された前記メディア鍵データ及び生成された前記暗号化コンテンツを前記記録媒体の前記書換可能領域に書き込み、

前記再生方法は、

前記記録媒体の前記書換可能領域に書き込まれたメディア鍵データから当該再生装置に対応する暗号化メディア鍵を読み出す読出ステップと、

当該再生装置のデバイス鍵を用いて、読み出された前記暗号化メディア鍵を復号して復号メディア鍵を生成する復号ステップと、

生成された復号メディア鍵が、前記検知情報であるか否かを判断し、前記検知情報である場合に、前記記録媒体に記録されている暗号化コンテンツの復号を禁止し、前記検知情報でない場合に、暗号化コンテンツの復号を許可する制御ステップと、

復号が許可された場合に、前記記録媒体から前記暗号化コンテンツを読み出し、生成された復号メディア鍵に基づいて、読み出した前記暗号化コンテンツを復号して復号コンテンツを生成する復号ステップと

を含むことを特徴とする再生方法。

３９．記録媒体にコンテンツを暗号化して書き込む記録装置と、前記記録媒体に記録されている暗号化コンテンツの復号を試みる複数の再生装置とから構成される著作物保護システムにおける前記再生装置で用いられる再生用のコンピュータプログラムであって、

前記複数の再生装置のうちいずれか１台以上は、無効化されており、

前記記録媒体は、読出専用の書換不可領域と、読出し及び書込みの可能な書換可能領域とを備え、前記書換不可領域には、当該記録媒体に固有の媒体固有番号が予め記録されており、

前記記録装置は、無効化されていない各再生装置についてメディア鍵が、無効化された各再生装置について所定の検知情報が、それぞれ、当該再生装置の

デバイス鍵を用いて、暗号化されて生成された複数の暗号化メディア鍵から構成されけるメディア鍵データを記憶しており、前記記録媒体の前記書換不可領域から前記媒体固有番号を読み出し、読み出した前記媒体固有番号及び前記メディア鍵に基づいて、暗号化鍵を生成し、生成された前記暗号化鍵に基づいて、デジタルデータであるコンテンツを暗号化して暗号化コンテンツを生成し、前記記憶手段から前記メディア鍵データを読み出し、読み出された前記メディア鍵データ及び生成された前記暗号化コンテンツを前記記録媒体の前記書換可能領域に書き込み、

前記再生用のコンピュータプログラムは、

前記記録媒体の前記書換可能領域に書き込まれたメディア鍵データから当該再生装置に対応する暗号化メディア鍵を読み出す読出ステップと、

当該再生装置のデバイス鍵を用いて、読み出された前記暗号化メディア鍵を復号して復号メディア鍵を生成する復号ステップと、

生成された復号メディア鍵が、前記検知情報であるか否かを判断し、前記検知情報である場合に、前記記録媒体に記録されている暗号化コンテンツの復号を禁止し、前記検知情報でない場合に、暗号化コンテンツの復号を許可する制御ステップと、

復号が許可された場合に、前記記録媒体から前記暗号化コンテンツを読み出し、生成された復号メディア鍵に基づいて、読み出した前記暗号化コンテンツを復号して復号コンテンツを生成する復号ステップと

を含むことを特徴とするコンピュータプログラム。

４０．前記コンピュータプログラムは、コンピュータ読み取り可能な記録媒体に記録されている

ことを特徴とする請求の範囲３９に記載のコンピュータプログラム。

４１．コンピュータ読み取り可能な記録媒体であって、

読出専用の書換不可領域と、読出し及び書込みの可能な書換可能領域とを備え、

前記書換不可領域には、当該記録媒体に固有の媒体固有番号が予め記録されており、

前記書換可能領域には、メディア鍵データと暗号化コンテンツとが記録され

ており、

前記メディア鍵データは、無効化されていない各再生装置についてメディア鍵が、無効化された各再生装置について所定の検知情報が、それぞれ、当該再生装置のデバイス鍵を用いて、暗号化されて生成された複数の暗号化メディア鍵から構成され、

前記暗号化コンテンツは、暗号化鍵に基づいて、デジタルデータであるコンテンツを暗号化して生成したものであり、

前記暗号化鍵は、前記記録媒体の前記書換不可領域に記録されている前記媒体固有番号及び前記メディア鍵に基づいて、生成されたものである

ことを特徴とする記録媒体。

４２．コンピュータ読み取り可能な記録媒体であって、

読出専用の書換不可領域と、読出し及び書込みの可能な書換可能領域とを備え、

前記書換不可領域には、当該記録媒体に固有の媒体固有番号が予め記録されており、

前記書換可能領域には、メディア鍵データと暗号化コンテンツとが記録されており、

前記メディア鍵データは、無効化されていない各再生装置についてメディア鍵が、無効化された各再生装置について所定の検知情報が、それぞれ、当該再生装置のデバイス鍵を用いて、暗号化されて生成された複数の暗号化メディア鍵から構成され、当該メディア鍵データを識別子するデータ識別子を含み、

前記暗号化コンテンツは、暗号化鍵に基づいて、デジタルデータであるコンテンツを暗号化して生成したものであり、前記データ識別子を含み、

前記暗号化鍵は、前記記録媒体の前記書換不可領域に記録されている前記媒体固有番号及び前記メディア鍵に基づいて、生成されたものである

ことを特徴とする記録媒体。

要 約 書

コンテンツの不正利用を防止することができる記録装置及び再生装置を提供する。

記録媒体は、書換不可領域に媒体固有番号を記録している。

記録装置は、メディア鍵データ及び暗号化コンテンツを前記記録媒体に書き込む。前記メディア鍵データは、無効化されていない各再生装置についてメディア鍵が、無効化された各再生装置について検知情報が、それぞれ、当該再生装置のデバイス鍵を用いて、暗号化されて生成された複数の暗号化メディア鍵から構成される。

再生装置は、デバイス鍵を用いて、暗号化メディア鍵を復号して復号メディア鍵を生成し、復号メディア鍵が、検知情報であるか否かを判断し、前記検知情報である場合に、前記記録媒体に記録されている暗号化コンテンツの復号を禁止する。